Traffic Management Shell (tmsh) Reference Guide

version 11.6.0

MAN-0306-09

Product Version

This manual applies to version 11.6.0 of the BIG-IP® product family.

Publication Date

This manual was published on August 8, 2014.

Legal Notices

Copyright

Copyright © 8/8/14, F5 Networks, Inc. All rights reserved.

F5 Networks, Inc. (F5) believes the information it furnishes to be accurate and reliable. However, F5 assumes no responsibility for the use of this information, nor any infringement of patents or other rights of third parties which may result from its use. No license is granted by implication or otherwise under any patent, copyright, or other intellectual property right of F5 except as specifically described by applicable user licenses. F5 reserves the right to change specifications at any time without notice.

Trademarks

AAM, Access Policy Manager, Advanced Client Authentication, Advanced Firewall Manager, Advanced Routing, AFM, Application Acceleration Manager, Application Security Manager, APM, ARX, AskF5, ASM, BIG-IP, BIG-IQ, Cloud Extender, CloudFucious, Cloud Manager, Clustered Multiprocessing, CMP, COHESION, Data Manager, DevCentral, DevCentral [DESIGN], DNS Express, DSC, DSI, Edge Client, Edge Gateway, Edge Portal, ELEVATE, EM, Enterprise Manager, ENGAGE, F5, F5 [DESIGN], F5 Certified [DESIGN], F5 Networks, F5 SalesXchange [DESIGN], F5 Synthesis, f5 Synthesis, F5 Synthesis [DESIGN], F5 TechXchange [DESIGN], Fast Application Proxy, Fast Cache, FirePass, Global Traffic Manager, GTM, GUARDIAN, iApps, IBR, iCall, Intelligent Browser Referencing, Intelligent Compression, IPv6 Gateway, iControl, iHealth, iQuery, iRules, iRules OnDemand, iSession, L7 Rate Shaping, LC, Link Controller, LineRate, LineRate Systems [DESIGN], Local Traffic Manager, LROS, LTM, Message Security Manager, MobileSafe, MSM, OneConnect, Packet Velocity, PEM, Policy Enforcement Manager, Protocol Security Manager, PSM, Real Traffic Policy Builder, SalesXchange, ScaleN, SDAC (except in Japan), SDC, Signalling Delivery Controller, Solutions for an application world, Software Designed Applications Services, SSL Acceleration, StrongBox, SuperVIP, SYN Check, TCP Express, TDR, TechXchange, TMOS, TotALL, Traffic Management Operating System, Traffix (except Germany), Traffix [DESIGN] (except Germany), Transparent Data Reduction, UNITY, VAULT, vCMP, VE F5 [DESIGN], Versafe, Versafe [DESIGN], VIPRION, Virtual Clustered Multiprocessing, WebSafe, and ZoneRunner, are trademarks or service marks of F5 Networks, Inc., in the U.S. and other countries, and may not be used without F5's express written consent.

All other product and company names herein may be trademarks of their respective owners.

Patents

This product may be protected by one or more patents indicated at:

http://www.f5.com/about/guidelines-policies/patents.

Export Regulation Notice

This product may include cryptographic software. Under the Export Administration Act, the United States government may consider it a criminal offense to export this product from the United States.

RF Interference Warning

This is a Class A product. In a domestic environment this product may cause radio interference, in which case the user may be required to take adequate measures.

FCC Compliance

This equipment has been tested and found to comply with the limits for a Class A digital device pursuant to Part 15 of FCC rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This unit generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference, in which case the user, at his own expense, will be required to take whatever measures may be required to correct the interference.

Any modifications to this device, unless expressly approved by the manufacturer, can void the user's authority to operate this equipment under part 15 of the FCC rules.

Canadian Regulatory Compliance

This class A digital apparatus complies with Canadian I CES-003.

Standards Compliance

This product conforms to the IEC, European Union, ANSI/UL and Canadian CSA standards applicable to Information Technology products at the time of manufacture.

Acknowledgments

This product includes software developed by Bill Paul.

This product includes software developed by Jonathan Stone.

This product includes software developed by Manuel Bouyer.

This product includes software developed by Paul Richards.

This product includes software developed by the NetBSD Foundation, Inc. and its contributors.

This product includes software developed by the Politecnico di Torino, and its contributors.

This product includes software developed by the Swedish Institute of Computer Science and its contributors.

This product includes software developed by the University of California, Berkeley and its contributors.

This product includes software developed by the Computer Systems Engineering Group at the Lawrence Berkeley Laboratory.

This product includes software developed by Christopher G. Demetriou for the NetBSD Project.

This product includes software developed by Adam Glass.

This product includes software developed by Christian E. Hopps.

This product includes software developed by Dean Huxley.

This product includes software developed by John Kohl.

This product includes software developed by Paul Kranenburg.

This product includes software developed by Terrence R. Lambert.

This product includes software developed by Philip A. Nelson.

This product includes software developed by Herb Peyerl.

This product includes software developed by Jochen Pohl for the NetBSD Project.

This product includes software developed by Chris Provenzano.

This product includes software developed by Theo de Raadt.

This product includes software developed by David Muir Sharnoff.

This product includes software developed by SigmaSoft, Th. Lockert.

This product includes software developed for the NetBSD Project by Jason R. Thorpe.

This product includes software developed by Jason R. Thorpe for And Communications, http://www.and.com.

This product includes software developed for the NetBSD Project by Frank Van der Linden.

This product includes software developed for the NetBSD Project by John M. Vinopal.

This product includes software developed by Christos Zoulas.

This product includes software developed by the University of Vermont and State Agricultural College and Garrett A. Wollman.

This product includes software developed by Balazs Scheidler (bazsi@balabit.hu), which is protected under the GNU Public License.

This product includes software developed by Niels Mueller (nisse@lysator.liu.se), which is protected under the GNU Public License.

In the following statement, "This software" refers to the Mitsumi CD-ROM driver: This software was developed by Holger Veit and Brian Moore for use with 386BSD and similar operating systems. "Similar operating systems" includes mainly non-profit oriented systems for research and education, including but not restricted to NetBSD, FreeBSD, Mach (by CMU).

This product includes software developed by the Apache Group for use in the Apache HTTP server project (http://www.apache.org/).

This product includes software licensed from Richard H. Porter under the GNU Library General Public License (© 1998, Red Hat Software), www.gnu.org/copyleft/lgpl.html.

This product includes the standard version of Perl software licensed under the Perl Artistic License (© 1997, 1998 Tom Christiansen and Nathan Torkington). All rights reserved. You may find the most current standard version of Perl at http://www.perl.com.

This product includes software developed by Jared Minch.

This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit (http://www.openssl.org/).

This product includes cryptographic software written by Eric Young (eay@cryptsoft.com).

This product contains software based on oprofile, which is protected under the GNU Public License.

This product includes software with glib library utility functions, which is protected under the GNU Public License.

This product includes software with grub2 bootloader functions, which is protected under the GNU Public License.

This product includes software with the Intel Gigabit Linux driver, which is protected under the GNU Public License. Copyright ©1999 - 2012 Intel Corporation.

This product includes software with the Intel 10 Gigabit PCI Express Linux driver, which is protected under the GNU Public License. Copyright ©1999 - 2012 Intel Corporation.

This product includes RRDtool software developed by Tobi Oetiker (http://www.rrdtool.com/index.html) and licensed under the GNU General Public License.

This product contains software licensed from Dr. Brian Gladman under the GNU General Public License (GPL).

This product includes software developed by the Apache Software Foundation (http://www.apache.org/).

This product includes Hypersonic SQL.

This product contains software developed by the Regents of the University of California, Sun Microsystems, Inc., Scriptics Corporation, and others.

This product includes software developed by the Internet Software Consortium.

This product includes software developed by Nominum, Inc. (http://www.nominum.com).

This product contains software developed by Broadcom Corporation, which is protected under the GNU Public License.

This product contains software developed by MaxMind LLC, and is protected under the GNU Lesser General Public License, as published by the Free Software Foundation.

This product includes software developed by Andrew Tridgell, which is protected under the GNU Public License, copyright ©1992-2000.

This product includes software developed by Jeremy Allison, which is protected under the GNU Public License, copyright ©1998.

This product includes software developed by Guenther Deschner, which is protected under the GNU Public License, copyright ©2008.

This product includes software developed by www.samba.org, which is protected under the GNU Public License, copyright ©2007.

This product includes software from Allan Jardine, distributed under the MIT License.

This product includes software from Trent Richardson, distributed under the MIT License.

This product includes vmbus drivers distributed by Microsoft Corporation.

This product includes software from Cavium.

This product includes software from Webroot, Inc.

This product includes software from Maxmind, Inc.

This product includes software from OpenVision Technologies, Inc. Copyright ©1993-1996, OpenVision Technologies, Inc. All Rights Reserved.

This product includes software developed by Matt Johnson, distributed under the MIT License. Copyright ©2012.

Permission is hereby granted, free of charge, to any person obtaining a copy of this software and associated documentation files (the "Software"), to deal in the Software without restriction, including without limitation the rights to use, copy, modify, merge, publish, distribute, sublicense, and/or sell copies of the Software, and to permit persons to whom the Software is furnished to do so, subject to the following conditions:

The above copyright notice and this permission notice shall be included in all copies or substantial portions of the Software.

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.

This product includes software from NLnetLabs. Copyright ©2001-2006. All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

- Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
- Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
- Neither the name of NLnetLabs nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT OWNER OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

This product includes GRand Unified Bootloader (GRUB) software developed under the GNU Public License, copyright ©2007.

This product includes Intel QuickAssist kernel module, library, and headers software licensed under the GNU General Public License (GPL).

This product includes gd-libgd library software developed by the following in accordance with the following copyrights:

- Portions copyright ©1994, 1995, 1996, 1997, 1998, 2000, 2001, 2002 by Cold Spring Harbor Laboratory. Funded under Grant P41-RR02188 by the National Institutes of Health.
- Portions copyright ©1996, 1997, 1998, 1999, 2000, 2001, 2002 by Boutell.Com, Inc.
- Portions relating to GD2 format copyright ©1999, 2000, 2001, 2002 Philip Warner.
- Portions relating to PNG copyright ©1999, 2000, 2001, 2002 Greg Roelofs.
- Portions relating to gdttf.c copyright ©1999, 2000, 2001, 2002 John Ellson (ellson@lucent.com).
- Portions relating to gdft.c copyright ©2001, 2002 John Ellson (ellson@lucent.com).
- Portions copyright ©2000, 2001, 2002, 2003, 2004, 2005, 2006, 2007 2008 Pierre-Alain Joye (pierre@libgd.org).
- Portions relating to JPEG and to color quantization copyright ©2000, 2001, 2002, Doug Becker and copyright ©1994, 1995, 1996, 1997, 1998, 1999, 2000, 2001, 2002, Thomas G. Lane. This software is based in part on the work of the Independent JPEG Group.
- Portions relating to WBMP copyright 2000, 2001, 2002 Maurice Szmurlo and Johan Van den Brande. Permission has been granted to copy, distribute and modify gd in any context without fee, including a commercial application, provided that this notice is present in user-accessible supporting documentation.

This product includes software developed by Oracle America, Inc. Copyright ©2012.

1. Java Technology Restrictions. Licensee shall not create, modify, change the behavior of, or authorize licensees of licensee to create, modify, or change the behavior of, classes, interfaces, or subpackages that are in any way identified as "java", "javax", "sun" or similar convention as specified by Oracle in any naming convention designation. In the event that Licensee creates an additional API(s) which: (a) extends the functionality of a Java Environment; and (b) is exposed to third party software developers for the purpose of developing additional software which invokes such additional API, Licensee must promptly publish broadly an accurate specification for such API for free use by all developer.
2. Trademarks and Logos. This License does not authorize an end user licensee to use any Oracle America, Inc. name, trademark, service mark, logo or icon. The end user licensee acknowledges that Oracle owns the Java trademark and all Java-related trademarks, logos and icon including the Coffee Cup and Duke ("Java Marks") and agrees to: (a) comply with the Java Trademark Guidelines at http://www.oraclc.com/html/3party.html; (b) not do anything harmful to or inconsistent with Oracle s rights in the Java Marks; and (c) assist Oracle in protecting those rights, including assigning to Oracle any rights acquired by Licensee in any Java Mark.
3. Source Code. Software may contain source code that, unless expressly licensed for other purposes, is provided solely for reference purposes pursuant to the terms of your license. Source code may not be redistributed unless expressly provided for in the terms of your license.
4. Third Party Code. Additional copyright notices and license terms applicable to portion of the Software are set forth in the THIRDPARTYLICENSEREADME.txt file.
5. Commercial Features. Use of the Commercial Features for any commercial or production purpose requires a separate license from Oracle. "Commercial Features" means those features identified in Table I-I (Commercial Features In Java SE Product Editions) of tile Software documentation accessible at http://www.oracle.com/technetwork/java/javase/documentation/index.html.

This product includes utilities developed by Linus Torvalds for inspecting devices connected to a USB bus.

This product includes perl-PHP-Serialization software, developed by Jesse Brown, copyright ©2003, and distributed under the Perl Development Artistic License (http://dev.perl.org/licenses/artistic.html).

This product includes software developed by members of the CentOS Project under the GNU Public License, copyright ©2004-2011 by the CentOS Project.

This product includes software licensed from Gerald Combs (gerald@wireshark.org) under the GNU General Public License as published by the Free Software Foundation; either version 2 of the License, or any later version. Copyright ©1998 Gerald Combs.

This product includes software licensed from Rémi Denis-Courmont under the GNU Library General Public License. Copyright ©2006 - 2011.

This product includes software developed by jQuery Foundation and other contributors, distributed under the MIT License. Copyright ©2014 jQuery Foundation and other contributors (http://jquery.com/).

Permission is hereby granted, free of charge, to any person obtaining a copy of this software and associated documentation files (the "Software"), to deal in the Software without restriction, including without limitation the rights to use, copy, modify, merge, publish, distribute, sublicense, and/or sell copies of the Software, and to permit persons to whom the Software is furnished to do so, subject to the following conditions:

The above copyright notice and this permission notice shall be included in all copies or substantial portions of the Software.

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.

This product includes software developed by Trent Richardson, distributed under the MIT License. Copyright ©2012 jQuery Foundation and other contributors (http://jquery.com/).

Permission is hereby granted, free of charge, to any person obtaining a copy of this software and associated documentation files (the "Software"), to deal in the Software without restriction, including without limitation the rights to use, copy, modify, merge, publish, distribute, sublicense, and/or sell copies of the Software, and to permit persons to whom the Software is furnished to do so, subject to the following conditions:

The above copyright notice and this permission notice shall be included in all copies or substantial portions of the Software.

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.

This product includes software developed by Allan Jardine, distributed under the MIT License. Copyright ©2008 - 2012, Allan Jardine, all rights reserved, jQuery Foundation and other contributors (http://jquery.com/).

Permission is hereby granted, free of charge, to any person obtaining a copy of this software and associated documentation files (the "Software"), to deal in the Software without restriction, including without limitation the rights to use, copy, modify, merge, publish, distribute, sublicense, and/or sell copies of the Software, and to permit persons to whom the Software is furnished to do so, subject to the following conditions:

The above copyright notice and this permission notice shall be included in all copies or substantial portions of the Software.

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.

This product includes software developed by Douglas Gilbert. Copyright ©1992 - 2012 The FreeBSD Project. All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.

2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

THIS SOFTWARE IS PROVIDED BY THE FREEBSD PROJECT "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO

EVENT SHALL THE FREEBSD PROJECT OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

The views and conclusions contained in the software and documentation are those of the authors and should not be interpreted as representing official policies, either expressed or implied, of the FreeBSD Project.

This product includes software developed as open source software. Copyright ©1994 - 2012 The FreeBSD Project. All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
3. The names of the authors may not be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED "AS IS" AND WITHOUT ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, WITHOUT LIMITATION, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE.

This product includes cryptographic software written by Eric Young (eay@cryptsoft.com). Copyright ©1998 - 2011 The OpenSSL Project. All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
3. All advertising materials mentioning features or use of this software must display the following acknowledgment: "This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit. (http://www.openssl.org/)"
4. The names "OpenSSL Toolkit" and "OpenSSL Project" must not be used to endorse or promote products derived from this software without prior written permission. For written permission, please contact openssl-core@openssl.org.
5. Products derived from this software may not be called "OpenSSL" nor may "OpenSSL" appear in their names without prior written permission of the OpenSSL Project.
6. Redistributions of any form whatsoever must retain the following acknowledgment: "This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit (http://www.openssl.org/)"

THIS SOFTWARE IS PROVIDED BY THE OpenSSL PROJECT "AS IS" AND ANY EXPRESSED OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE OpenSSL PROJECT OR ITS CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

This product includes software licensed from William Ferrell, Selene Scriven and many other contributors under the GNU General Public License, copyright ©1998 - 2006.

This product includes software developed by Thomas Williams and Colin Kelley. Copyright ©1986 - 1993, 1998, 2004, 2007

Permission to use, copy, and distribute this software and its documentation for any purpose with or without fee is hereby granted, provided that the above copyright notice appear in all copies and that both that copyright notice and this permission notice appear in supporting documentation. Permission to modify the software is granted, but not the right to distribute the complete modified source code. Modifications are to be distributed as patches to the released version. Permission to distribute binaries produced by compiling modified sources is granted, provided you

1. distribute the corresponding source modifications from the released version in the form of a patch file along with the binaries,
2. add special version identification to distinguish your version in addition to the base release version number,
3. provide your name and address as the primary contact for the support of your modified version, and
4. retain our contact information in regard to use of the base software.

Permission to distribute the released version of the source code along with corresponding source modifications in the form of a patch file is granted with same provisions 2 through 4 for binary distributions. This software is provided "as is" without express or implied warranty to the extent permitted by applicable law.

This product includes software developed by the Computer Systems Engineering Group at Lawrence Berkeley Laboratory. Copyright ©1990-1994 Regents of the University of California. All rights reserved. Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
3. All advertising materials mentioning features or use of this software must display the following acknowledgment: This product includes software developed by the Computer Systems Engineering Group at Lawrence Berkeley Laboratory.
4. Neither the name of the University nor of the Laboratory may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE REGENTS AND CONTRIBUTORS "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE REGENTS OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

This product includes software developed by Sony Computer Science Laboratories Inc. Copyright © 1997-2003 Sony Computer Science Laboratories Inc. All rights reserved. Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

THIS SOFTWARE IS PROVIDED BY SONY CSL AND CONTRIBUTORS "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL SONY CSL OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR

SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

This product contains software developed by Google, Inc. Copyright ©2011 Google, Inc.

Permission is hereby granted, free of charge, to any person obtaining a copy of this software and associated documentation files (the "Software"), to deal in the Software without restriction, including without limitation the rights to use, copy, modify, merge, publish, distribute, sublicense, and/or sell copies of the Software, and to permit persons to whom the Software is furnished to do so, subject to the following conditions:

The above copyright notice and this permission notice shall be included in all copies or substantial portions of the Software.

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.

This product includes software developed by Jeremy Ashkenas and DocumentCloud, and distributed under the MIT license. Copyright © 2010-2013 Jeremy Ashkenas, DocumentCloud.

This product includes gson software, distributed under the Apache License version 2.0. Copyright © 2008-2011 Google Inc.

This product includes ec2-tools software, copyright © 2008, Amazon Web Services, and licensed under the Amazon Software License. A copy of the License is located at http://aws.amazon.com/asl/ .

This product includes the ixgbevf Intel Gigabit Linux driver, Copyright © 1999 - 2012 Intel Corporation, and distributed under the GPLv2 license, as published by the Free Software Foundation.

This product includes libwebp software. Copyright © 2010, Google Inc. All rights reserved.

This product includes Angular software developed by Google, Inc., http://angularjs.org, copyright © 2010-2012 Google, Inc., and distributed under the MIT license.

This product includes node.js software, copyright © Joyent, Inc. and other Node contributors. All rights reserved.

Permission is hereby granted, free of charge, to any person obtaining a copy of this software and associated documentation files (the "Software"), to deal in the Software without restriction, including without limitation the rights to use, copy, modify, merge, publish, distribute, sublicense, and/or sell copies of the Software, and to permit persons to whom the Software is furnished to do so, subject to the following conditions:

- The above copyright notice and this permission notice shall be included in all copies or substantial portions of the Software.

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.

This product includes bootstrap software, copyright © 2011-2014 Twitter, Inc., and distributed under the MIT license (http://getbootstrap.com/getting-started/#license-faqs).

This product includes Intel PCM software, copyright © 2009-2013, Intel Corporation All rights reserved. This software is distributed under the OSI BSD license.

This product includes jxrlib software, copyright ©2009 Microsoft Corp. All rights reserved. Distributed under the new BSD license.

This product includes Net-SNMP software, to which one or more of the following copyrights apply:

- Copyright © 1989, 1991, 1992 by Carnegie Mellon University; Derivative Work - 1996, 1998-2000, Copyright © 1996, 1998-2000, The Regents of the University of California. All rights reserved. Distributed under CMU/UCD license (BSD like).
- Copyright © 2001-2003, Networks Associates Technology, Inc. All rights reserved. Distributed under the BSD license.
- Portions of this code are copyright © 2001-2003, Cambridge Broadband Ltd. All rights reserved. Distributed under the BSD license.
- Copyright © 2003 Sun Microsystems, Inc., 4150 Network Circle, Santa Clara, California 95054, U.S.A. All rights reserved. Distributed under the BSD license.
- Copyright © 2003-2009, Sparta, Inc. All rights reserved. Distributed under the BSD license.
- Copyright © 2004, Cisco, Inc and Information Network Center of Beijing University of Posts and Telecommunications. All rights reserved. Distributed under the BSD license.
- Copyright © 2003Fabasoft R&D Software GmbH & Co KG, oss@fabasoft.com. Distributed under the BSD license.
- Copyright © 2007 Apple Inc. All rights reserved. Distributed under the BSD license.
- Copyright © 2009 ScienceLogic, Inc. All rights reserved. Distributed under the BSD license.

This product includes Racoon 2 software, copyright © 2003-2005 WIDE Project. All rights reserved. Distributed under a BSD-like license.

This product includes node-uuid software, copyright © 2010-2012, Robert Kieffer, and distributed under the MIT license.

This product includes opencsv software, which is distributed under the Apache 2.0 license.

This product includes owasp-jave-encoder software, copyright © 2014, Jeff Ichnowski, and distributed under the New BSD license.

This product may include Intel SDD software subject to the following license; check your hardware specification for details.

1. LICENSE. This Software is licensed for use only in conjunction with Intel solid state drive (SSD) products. Use of the Software in conjunction with non-Intel SSD products is not licensed hereunder. Subject to the terms of this Agreement, Intel grants to You a nonexclusive, nontransferable, worldwide, fully paid-up license under Intel s copyrights to:
   - copy the Software onto a single computer or multiple computers for Your personal, noncommercial use; and
   - make appropriate back-up copies of the Software, for use in accordance with Section 1a) above.

   The Software may contain the software or other property of third party suppliers, some of which may be identified in, and licensed in accordance with, any enclosed "license.txt" file or other text or file.

   Except as expressly stated in this Agreement, no license or right is granted to You directly or by implication, inducement, estoppel or otherwise. Intel will have the right to inspect or have an independent auditor inspect Your relevant records to verify Your compliance with the terms and conditions of this Agreement.
2. RESTRICTIONS. You will not:
   - copy, modify, rent, sell, distribute or transfer any part of the Software, and You agree to prevent unauthorized copying of the Software; and,
   - reverse engineer, decompile, or disassemble the Software; and,
   - sublicense or permit simultaneous use of the Software by more than one user; and,
   - otherwise assign, sublicense, lease, or in any other way transfer or disclose Software to any third party, except as set forth herein; and,
   - subject the Software, in whole or in part, to any license obligations of Open Source Software including without limitation combining or distributing the Software with Open Source Software in a manner that subjects the Software or any portion of the Software provided by Intel hereunder to any license obligations of such Open Source Software. "Open Source Software" means any software that requires as a condition of use, modification and/or distribution of such software that such software or other software incorporated into, derived from or distributed with such software:
   - be disclosed or distributed in source code form; or

- be licensed by the user to third parties for the purpose of making and/or distributing derivative works; or
- be redistributable at no charge.

Open Source Software includes, without limitation, software licensed or distributed under any of the following licenses or distribution models, or licenses or distribution models substantially similar to any of the following:

- GNU's General Public License (GPL) or Lesser/Library GPL (LGPL),
- the Artistic License (e.g., PERL),
- the Mozilla Public License,
- the Netscape Public License,
- the Sun Community Source License (SCSL),
- vi) the Sun Industry Source License (SISL),
- vii) the Apache Software license, and
- viii) the Common Public License (CPL).

3. OWNERSHIP OF SOFTWARE AND COPYRIGHTS. Title to all copies of the Software remains with Intel or its suppliers. The Software is copyrighted and protected by the laws of the United States and other countries, and international treaty provisions. You may not remove any copyright notices from the Software. Intel may make changes to the Software, or to materials referenced therein, at any time and without notice, but is not obligated to support or update the Software. Except as otherwise expressly provided, Intel grants no express or implied right or license under Intel patents, copyrights, trademarks, or other intellectual property rights.

4. Entire Agreement. This Agreement contains the complete and exclusive statement of the agreement between You and Intel and supersedes all proposals, oral or written, and all other communications relating to the subject matter of this Agreement. Only a written instrument duly executed by authorized representatives of Intel and You may modify this Agreement.

5. LIMITED MEDIA WARRANTY. If the Software has been delivered by Intel on physical media, Intel warrants the media to be free from material physical defects for a period of ninety (90) days after delivery by Intel. If such a defect is found, return the media to Intel for replacement or alternate delivery of the Software as Intel may select.

6. EXCLUSION OF OTHER WARRANTIES. EXCEPT AS PROVIDED ABOVE, THE SOFTWARE IS PROVIDED "AS IS" WITHOUT ANY EXPRESS OR IMPLIED WARRANTY OF ANY KIND, INCLUDING WARRANTIES OF MERCHANTABILITY, NONINFRINGEMENT, OR FITNESS FOR A PARTICULAR PURPOSE. Intel does not warrant or assume responsibility for any errors, the accuracy or completeness of any information, text, graphics, links or other materials contained within the Software.

7. LIMITATION OF LIABILITY. IN NO EVENT WILL INTEL OR ITS SUPPLIERS BE LIABLE FOR ANY DAMAGES WHATSOEVER (INCLUDING, WITHOUT LIMITATION, LOST PROFITS, BUSINESS INTERRUPTION OR LOST INFORMATION) ARISING OUT OF THE USE OF OR INABILITY TO USE THE SOFTWARE, EVEN IF INTEL HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. SOME JURISDICTIONS PROHIBIT EXCLUSION OR LIMITATION OF LIABILITY FOR IMPLIED WARRANTIES OR CONSEQUENTIAL OR INCIDENTAL DAMAGES, SO THE ABOVE LIMITATION MAY NOT APPLY TO YOU. YOU MAY ALSO HAVE OTHER LEGAL RIGHTS THAT VARY FROM JURISDICTION TO JURISDICTION.

8. TERMINATION OF THIS AGREEMENT. Intel may terminate this Agreement at any time if You violate its terms. Upon termination, You will immediately destroy the Software or return all copies of the Software to Intel.

9. APPLICABLE LAWS. Claims arising under this Agreement will be governed by the laws of Delaware, excluding its principles of conflict of laws and the United Nations Convention on Contracts for the Sale of Goods. You may not export the Software in violation of applicable export laws and regulations. Intel is not obligated under any other agreements unless they are in writing and signed by an authorized representative of Intel.

10. GOVERNMENT RESTRICTED RIGHTS. The Software is provided with "RESTRICTED RIGHTS." Use, duplication, or disclosure by the Government is subject to restrictions as set forth in FAR52.227-14 and DFAR252.227-7013 et seq. or their successors. Use of the Software by the

Government constitutes acknowledgment of Intel s proprietary rights therein. Contractor or Manufacturer is Intel Corporation, 2200 Mission College Blvd., Santa Clara, CA 95054.

Table of Contents

1
Introducing the Traffic Management Shell

About the Traffic Management Shell 1-1
Additional command line utilities and tools 1-2
Basic syntax conventions 1-3

2
Understanding and Using the Traffic Management Shell

Understanding the structure of tmsh 2-1
Using tmsh 2-2
- Loading and saving the system configuration 2-2
- Working within the tmsh hierarchy 2-3
- Using the scripting feature 2-6
- Using the command completion feature 2-7
- Using the help feature 2-9
- Using the context-sensitive help feature 2-10
- Interrupting a command 2-10
- Entering multiple commands 2-10
- Using the command glob feature 2-11
- Using the command audit feature 2-15
- Using the command aliases feature 2-17
- Using the wildcard search feature 2-19
- Using the statistics feature 2-19
- Using grep functionality in tmsh to filter output 2-22
- Creating batch mode transactions 2-23
- Controlling tmsh 2-24

Introduction to command syntax 2-27

3
Global Commands

Introducing global commands 3-1
Alphabetical list of global commands 3-1
cd 3-2
cp 3-4
create 3-6
delete 3-7
edit 3-9
exit 3-11
generate 3-12
help 3-13
install 3-15
list 3-16
load 3-19
modify 3-20
mv 3-22
publish 3-24
pwd 3-25
quit 3-26
reboot 3-27
reset-stats 3-29
restart 3-31
run 3-32
save 3-35
send-mail 3-36

show 3-37
shutdown 3-41
start 3-42
stop 3-43
submit 3-44
time 3-45
tmsh 3-48

4
analytics
Introducing the analytics module 4-1
Alphabetical list of components 4-1
report 4-2

5
analytics application-security
Introducing the analytics application-security module 5-1
Alphabetical list of components 5-1
report 5-2
scheduled-report 5-7

6
analytics application-security-network
Introducing the analytics application-security-network module 6-1
Alphabetical list of components 6-1
report 6-2

7
analytics application-security-anomalies
Introducing the analytics application-security-anomalies module 7-1
Alphabetical list of components 7-1
report 7-2

8
analytics cpu
Introducing the analytics cpu module 8-1
Alphabetical list of components 8-1
report 8-2

9
analytics disk-info
Introducing the analytics disk-info module 9-1
Alphabetical list of components 9-1
report 9-2

10
analytics dns
Introducing the analytics dns module 10-1
Alphabetical list of components 10-1
report 10-2

11
analytics dns-dos
Introducing the analytics dns-dos module 11-1
Alphabetical list of components 11-1
report 11-2

12
analytics dns-protocol
Introducing the analytics dns-protocol module 12-1
Alphabetical list of components 12-1
report 12-2

13
analytics dos-l3
Introducing the analytics dos-l3 module 13-1
Alphabetical list of components 13-1
report 13-2

14
analytics dos-l7
Introducing the analytics dos-l7 module 14-1
Alphabetical list of components 14-1
report 14-2

15
analytics http
Introducing the analytics http module 15-1
Alphabetical list of components 15-1
report 15-2

16
analytics ip-layer
Introducing the analytics ip-layer module 16-1
Alphabetical list of components 16-1
report 16-2

17
analytics memory
Introducing the analytics memory module 17-1
Alphabetical list of components 17-1
report 17-2

18
analytics network
Introducing the analytics network module 18-1
Alphabetical list of components 18-1
report 18-2
stale-rules 18-10

19
analytics pem
Introducing the analytics pem module 19-1
Alphabetical list of components 19-1
report 19-2

20
analytics protocol-security
Introducing the analytics protocol-security module 20-1
Alphabetical list of components 20-1
report 20-2

21
analytics sip-dos
Introducing the analytics sip-dos module 21-1
Alphabetical list of components 21-1
report 21-2

22
analytics swg
Introducing the analytics swg module 22-1
Alphabetical list of components 22-1
report 22-2

23
analytics swg-blocked
Introducing the analytics swg-blocked module 23-1
Alphabetical list of components 23-1
report 23-2

24
analytics tcp
Introducing the analytics tcp module 24-1
Alphabetical list of components 24-1
report 24-2

25
analytics udp
Introducing the analytics udp module 25-1
Alphabetical list of components 25-1
report 25-2

26
analytics vcmp
Introducing the analytics vcmp module 26-1
Alphabetical list of components 26-1
report 26-2

27
analytics virtual

Introducing the analytics virtual module 27-1
Alphabetical list of components 27-1
report 27-2

28
apm

Introducing the apm module 28-1
Alphabetical list of components 28-1
acl 28-2
apm-avr-config 28-6
log-setting 28-7
swg-scheme 28-9
url-filter 28-11

29
apm aaa

Introducing the apm aaa module 29-1
Alphabetical list of components 29-1
active-directory 29-2
active-directory-trusted-domains 29-5
crldp 29-7
http 29-10
kerberos 29-14
kerberos-keytab-file 29-16
ldap 29-18
oam 29-22
ocsp 29-26
radius 29-30
saml 29-33
saml-idp-connector 29-37
securid 29-41
tacacsplus 29-43

30
apm epsec

Introducing the apm epsec module 30-1
Alphabetical list of components 30-1
epsec-package 30-2
software-status 30-4

31
apm mam

Introducing the apm mam module 31-1
Alphabetical list of components 31-1
idbridge 31-2
mam-server 31-4

32
apm mam scim-config

Introducing the apm mam scim-config module 32-1
Alphabetical list of components 32-1
scim-config 32-2

33
apm ntlm

Introducing the apm ntlm module 33-1
Alphabetical list of components 33-1
machine-account 33-2
ntlm-auth 33-5

34
apm policy

Introducing the apm policy module 34-1
Alphabetical list of components 34-1
access-policy 34-2
customization-group 34-3
image-file 34-4
policy-item 34-5
Warning: This page is obsolete. Windows Group Policy is no longer supported.
windows-group-policy-file - Manages FullArmor GPAnywhere Windows group policy files. 34-6

35
apm policy agent

Introducing the apm policy agent module 35-1
Alphabetical list of components 35-1
aaa-active-directory 35-2
aaa-client-cert 35-5
aaa-crldp 35-7
aaa-http 35-9
aaa-ldap 35-11
aaa-ocsp 35-16
aaa-radius 35-18
aaa-securid 35-20
acct-radius 35-22
acct-tacacsplus 35-24
decision-box 35-26
dynamic-acl 35-28
ending-allow 35-30
ending-deny 35-32
ending-redirect 35-34
endpoint-check-machine-cert 35-36
endpoint-check-software 35-39
endpoint-linux-check-file 35-44
endpoint-linux-check-process 35-47
endpoint-mac-check-file 35-50
endpoint-mac-check-process 35-53
endpoint-machine-info 35-55
endpoint-windows-browser-cache-cleaner 35-57
endpoint-windows-check-file 35-60

endpoint-windows-check-process 35-63
endpoint-windows-check-registry 35-66
Warning: This page is obsolete. Windows Group Policy is no longer supported.
endpoint-windows-group-policy - Manages an Endpoint Windows Group Policy agent. ... 35-69
endpoint-windows-info-os 35-71
endpoint-windows-protected-workspace 35-73
external-logon-page 35-75
irule-event 35-77
kerberos 35-79
logging 35-81
logon-page 35-83
message-box 35-87
oam 35-89
resource-assign 35-91
route-domain-selection 35-93
tacacsplus 35-95
variable-assign 35-97

36
apm profile

Introducing the apm profile module 36-1
Alphabetical list of components 36-1
access 36-2
connectivity 36-9
exchange 36-14
remote-desktop 36-17
vdi 36-18

37
apm resource

Introducing the apm resource module 37-1
Alphabetical list of components 37-1
app-tunnel 37-2
client-rate-class 37-5
client-traffic-classifier 37-8
ipv6-leasepool 37-11
leasepool 37-13
network-access 37-15
portal-access 37-23
sandbox 37-26
webtop 37-29
webtop-link 37-32

38
apm resource remote-desktop

Introducing the apm resource remote-desktop module 38-1
Alphabetical list of components 38-1
citrix 38-2
citrix-client-bundle 38-5
citrix-client-package-file 38-7
quest 38-9
rdp 38-12

vmware-view 38-18

39
apm saml

Introducing the apm saml module 39-1
Alphabetical list of components 39-1
artifact-resolution-service 39-2

40
apm sso

Introducing the apm sso module 40-1
Alphabetical list of components 40-1
basic 40-2
form-based 40-5
form-basedv2 40-8
kerberos 40-17
ntlmv1 40-21
ntlmv2 40-24
saml 40-27
saml-resource 40-31
saml-sp-connector 40-33

41
asm

Introducing the asm module 41-1
Alphabetical list of components 41-1
device-sync 41-2
http-method 41-3
httpclass-asm 41-5
policy 41-7
predefined-policy 41-11
response-code 41-12
webapp-language 41-14

42
auth

Introducing the auth module 42-1
Alphabetical list of components 42-1
apm-auth 42-2
cert-ldap 42-4
ldap 42-9
login-failures 42-14
partition 42-16
password 42-18
password-policy 42-19
radius 42-22
radius-server 42-25
remote-role 42-28
remote-user 42-32
source 42-34
tacacs 42-36
user 42-39

43
cli

Introducing the cli module 43-1
Alphabetical list of components 43-1
admin-partitions 43-2
global-settings 43-3
history 43-5
preference 43-6
script 43-12
transaction 43-31
version 43-34

44
cli alias

Introducing the cli alias module 44-1
Alphabetical list of components 44-1
private 44-2
shared 44-5

45
cm

Introducing the cm module 45-1
Alphabetical list of components 45-1
cert 45-2
config-sync 45-5
device 45-7
device-group 45-11
failover-status 45-15
key 45-16
sniff-updates 45-19
sync-status 45-20
traffic-group 45-21
trust-domain 45-24
watch-devicegroup-device 45-28
watch-sys-device 45-30
watch-trafficgroup-device 45-32

46
gtm

Introducing the gtm module 46-1
Alphabetical list of components 46-1
datacenter 46-2
distributed-app 46-5
iquery 46-9
ldns 46-10
link 46-11
listener 46-16
path 46-22
persist 46-23
pool 46-25
prober-pool 46-37
region 46-41
rule 46-44

server 46-47
topology 46-55
traffic 46-58
wideip 46-59

47
gtm global-settings

Introducing the gtm global-settings module 47-1
Alphabetical list of components 47-1
general 47-2
load-balancing 47-6
metrics 47-8
metrics-exclusions 47-11

48
gtm monitor

Introducing the gtm monitor module 48-1
Alphabetical list of components 48-1
bigip 48-2
bigip-link 48-6
external 48-9
firepass 48-12
ftp 48-16
gateway-icmp 48-20
gtp 48-23
http 48-26
https 48-30
imap 48-34
ldap 48-38
mssql 48-42
mysql 48-46
nntp 48-50
oracle 48-54
pop3 48-58
postgresql 48-61
radius 48-65
radius-accounting 48-69
real-server 48-73
scripted 48-76
sip 48-79
smtp 48-84
snmp 48-87
snmp-link 48-91
soap 48-95
tcp 48-99
tcp-half-open 48-103
udp 48-106
wap 48-110
wmi 48-114

49
ltm

Introducing the ltm module 49-1

Alphabetical list of components 49-1
alg-log-profile 49-2
default-node-monitor 49-5
eviction-policy 49-7
ifile 49-13
lsn-log-profile 49-15
lsn-pool 49-18
nat 49-25
node 49-28
policy 49-33
policy-strategy 49-44
pool 49-48
rule 49-60
snat 49-64
snat-translation 49-68
snatpool 49-71
traffic-class 49-73
virtual 49-76
virtual-address 49-89

50
ltm auth

Introducing the ltm auth module 50-1
Alphabetical list of components 50-1
crldp-server 50-2
kerberos-delegation 50-5
ldap 50-8
ocsp-responder 50-13
profile 50-18
radius 50-21
radius-server 50-24
ssl-cc-ldap 50-27
ssl-crldp 50-32
ssl-ocsp 50-35
tacacs 50-38

51
ltm classification

Introducing the ltm classification module 51-1
Alphabetical list of components 51-1
application 51-2
category 51-4
http-signature 51-6
key 51-9
policy 51-11
signature-definition 51-13
signature-update-schedule 51-15
signature-version 51-17
signatures 51-19
update-signatures 51-20
url-category 51-21
urldb-feed-list 51-23
urldb-file 51-25

52
ltm classification stats

Introducing the ltm classification stats module 52-1
Alphabetical list of components 52-1
application 52-2
url-category 52-4

53
ltm clientssl

Introducing the ltm clientssl module 53-1
Alphabetical list of components 53-1
ocsp-stapling-responses 53-2

54
ltm clientssl-proxy

Introducing the ltm clientssl-proxy module 54-1
Alphabetical list of components 54-1
cached-certs 54-2

55
ltm data-group

Introducing the ltm data-group module 55-1
Alphabetical list of components 55-1
external 55-2
internal 55-6

56
ltm dns

Introducing the ltm dns module 56-1
Alphabetical list of components 56-1
dns-express-db 56-2
nameserver 56-3
tsig-key 56-5
zone 56-7

57
ltm dns analytics

Introducing the ltm dns analytics module 57-1
Alphabetical list of components 57-1
global-settings 57-2

58
ltm dns cache

Introducing the ltm dns cache module 58-1
Alphabetical list of components 58-1
global-settings 58-2
resolver 58-4
transparent 58-10
validating-resolver 58-14

59
ltm dns cache records

Introducing the ltm dns cache records module 59-1
Alphabetical list of components 59-1
key 59-2
msg 59-4
nameserver 59-6
rrset 59-8

60
ltm dns dnssec

Introducing the ltm dns dnssec module 60-1
Alphabetical list of components 60-1
generation 60-2
key 60-4
zone 60-8

61
ltm global-settings

Introducing the ltm global-settings module 61-1
Alphabetical list of components 61-1
connection 61-2
general 61-4
traffic-control 61-6

62
ltm message-routing generic

Introducing the ltm message-routing generic module 62-1
Alphabetical list of components 62-1
peer 62-2
protocol 62-4
route 62-6
router 62-8
transport-config 62-11

63
ltm message-routing sip

Introducing the ltm message-routing sip module 63-1
Alphabetical list of components 63-1
peer 63-2
route 63-4
transport-config 63-7

64
ltm message-routing sip profile

Introducing the ltm message-routing sip profile module 64-1
Alphabetical list of components 64-1
router 64-2
session 64-5

65
ltm monitor

Introducing the ltm monitor module 65-1
Alphabetical list of components 65-1
diameter 65-2
dns 65-7
external 65-13
firepass 65-17
ftp 65-21
gateway-icmp 65-26
http 65-30
https 65-36
icmp 65-42
imap 65-46
inband 65-50
ldap 65-53
module-score 65-58
mssql 65-62
mysql 65-67
nntp 65-72
oracle 65-76
pop3 65-81
postgresql 65-85
radius 65-90
radius-accounting 65-94
real-server 65-98
rpc 65-101
sasp 65-105
scripted 65-108
sip 65-112
smb 65-117
smtp 65-121
snmp-dca 65-125
snmp-dca-base 65-129
soap 65-132
tcp 65-137
tcp-echo 65-142
tcp-half-open 65-146
udp 65-150
virtual-location 65-156
wap 65-160
wmi 65-165

66
ltm persistence

Introducing the ltm persistence module 66-1
Alphabetical list of components 66-1
cookie 66-2
dest-addr 66-6
global-settings 66-10
hash 66-12
msrdp 66-16
persist-records 66-19
sip 66-22

source-addr 66-25
ssl 66-29
universal 66-32

67
ltm profile

Introducing the ltm profile module 67-1
Alphabetical list of components 67-1
analytics 67-2
certificate-authority 67-11
classification 67-13
client-ldap 67-15
client-ssl 67-17
dhcpv4 67-30
dhcpv6 67-36
diameter 67-41
dns 67-46
dns-logging 67-50
fasthttp 67-53
fastl4 67-58
fix 67-65
ftp 67-68
html 67-71
http 67-74
http-compression 67-84
http2 67-89
icap 67-92
iiop 67-95
ipother 67-98
mblb 67-100
mssql 67-103
ntlm 67-106
ocsp-stapling-params 67-109
one-connect 67-112
pcp 67-116
pptp 67-120
qoe 67-122
radius 67-124
ramcache 67-127
request-adapt 67-129
request-log 67-132
response-adapt 67-136
rewrite 67-139
rtsp 67-144
sctp 67-148
server-ldap 67-152
server-ssl 67-154
sip 67-164
smtp 67-169
smtps 67-171
socks 67-173
spdy 67-176
statistics 67-180
stream 67-183
tcp 67-186

udp 67-196
wa-cache 67-199
web-acceleration 67-200
web-security 67-204
xml 67-206

68
net

Introducing the net module 68-1
Alphabetical list of components 68-1
arp 68-2
bwc-policy 68-5
cmetrics 68-14
ike-evt-stat 68-16
ike-msg-stat 68-17
interface 68-18
interface-cos 68-24
ndp 68-25
packet-filter 68-27
packet-filter-trusted 68-32
port-mirror 68-35
route 68-37
route-domain 68-40
router-advertisement 68-47
rst-cause 68-51
self 68-52
self-allow 68-59
stp 68-61
stp-globals 68-65
trunk 68-68
vlan 68-73
vlan-allowed 68-78
vlan-group 68-79
wccp 68-83

69
net cos

Introducing the net cos module 69-1
Alphabetical list of components 69-1
global-settings 69-2
map-8021p 69-4
map-dscp 69-6
traffic-priority 69-8

70
net dns-resolver

Introducing the net dns-resolver module 70-1
Alphabetical list of components 70-1
resolver 70-2

71
net fdb

Introducing the net fdb module 71-1

Alphabetical list of components 71-1
tunnel 71-2
vlan 71-4

72
net ipsec

Introducing the net ipsec module 72-1
Alphabetical list of components 72-1
ike-daemon 72-2
ike-peer 72-4
ike-sa 72-9
ipsec-policy 72-10
ipsec-sa 72-14
manual-security-association 72-16
traffic-selector 72-19

73
net rate-shaping

Introducing the net rate-shaping module 73-1
Alphabetical list of components 73-1
class 73-2
drop-policy 73-6
queue 73-9
shaping-policy 73-12

74
net tunnels

Introducing the net tunnels module 74-1
Alphabetical list of components 74-1
etherip 74-2
fec 74-4
gre 74-7
ipip 74-10
ipsec 74-12
map 74-14
ppp 74-16
tunnel 74-19
v6rd 74-22
vxlan 74-25
wccp 74-27

75
pem

Introducing the PEM module 75-1
Alphabetical list of components 75-1
forwarding-endpoint 75-2
interception-endpoint 75-6
irule 75-8
listener 75-11
policy 75-13
service-chain-endpoint 75-24
sessiondb 75-28
subscriber 75-31

subscribers 75-34

76
pem global-settings

Introducing the PEM global-settings module 76-1
Alphabetical list of components 76-1
analytics 76-2
quota-mgmt 76-4
subscriber-activity-log 76-6

77
pem profile

Introducing the PEM profile module 77-1
Alphabetical list of components 77-1
diameter-endpoint 77-2
radius-aaa 77-5
spm 77-7

78
pem quota management

Introducing the PEM quota management module 78-1
Alphabetical list of components 78-1
rating-group 78-2

79
pem reporting

Introducing the PEM Reporting module 79-1
Alphabetical list of components 79-1
format-script 79-2

80
pem stats

Introducing the PEM stats module 80-1
Alphabetical list of components 80-1
action 80-2
gx 80-5
gy 80-8
hsl 80-11
radius 80-13
subscriber 80-15

81
security analytics

Introducing the security analytics module 81-1
Alphabetical list of components 81-1
settings 81-2

82
security anti-fraud

Introducing the security anti-fraud module 82-1

Alphabetical list of components 82-1
profile 82-2

83
security datasync

Introducing the security datasync module 83-1
Alphabetical list of components 83-1
device-stats 83-2
global-profile 83-3
local-profile 83-6

84
security dos

Introducing the security dos module 84-1
Alphabetical list of components 84-1
device-config 84-2
network-whitelist 84-10
profile 84-14
udp-portlist 84-28

85
security firewall

Introducing the security firewall module 85-1
Alphabetical list of components 85-1
address-list 85-2
global-rules 85-5
management-ip-rules 85-14
matching-rule 85-22
policy 85-23
port-list 85-28
rule-list 85-31
rule-stat 85-40
schedule 85-41
user-domain 85-44
user-list 85-46

86
security http

Introducing the security http module 86-1
Alphabetical list of components 86-1
file-type 86-2
mandatory-header 86-3
profile 86-4

87
security ip-intelligence

Introducing the security ip-intelligence module 87-1
Alphabetical list of components 87-1
blacklist-category 87-2
feed-list 87-4
global-policy 87-8
info 87-10

policy 87-12

88
security log

Introducing the security log module 88-1
Alphabetical list of components 88-1
network-storage-field 88-2
profile 88-3
protocol-dns-storage-field 88-18
protocol-sip-storage-field 88-19
remote-format 88-20
storage-field 88-22

89
sys

Introducing the sys module 89-1
Alphabetical list of components 89-1
clock 89-2
cluster 89-3
config 89-5
config-diff 89-11
connection 89-12
console 89-15
cpu 89-16
daemon-ha 89-17
datastor 89-20
db 89-22
default-config 89-25
dns 89-26
failover 89-28
feature-module 89-31
fix-connection 89-33
folder 89-34
geoip 89-37
global-settings 89-38
ha-group 89-43
ha-status 89-46
hardware 89-47
host-info 89-48
httpd 89-49
hypervisor-info 89-55
icmp-stat 89-56
ip-address 89-57
ip-stat 89-59
iprep-status 89-60
license 89-62
log 89-64
log-rotate 89-66
mac-address 89-69
management-dhcp 89-71
management-ip 89-73
management-route 89-75
mcp-state 89-78
memory 89-79

ntp 89-80
outbound-smtp 89-84
proc-info 89-86
provision 89-87
pva-traffic 89-91
scriptd 89-93
service 89-95
smtp-server 89-97
snmp 89-99
sshd 89-113
state-mirroring 89-116
sync-sys-files 89-118
syslog 89-119
tmm-info 89-123
tmm-traffic 89-124
traffic 89-125
ucs 89-126
version 89-128

90
sys application

Introducing the sys application module 90-1
Alphabetical list of components 90-1
apl-script 90-2
custom-stat 90-5
service 90-7
template 90-10

91
sys crypto

Introducing the sys crypto module 91-1
Alphabetical list of components 91-1
cert 91-2
check-cert 91-5
client 91-7
crl 91-9
key 91-11
master-key 91-15
pkcs12 91-17
server 91-19

92
sys crypto fips

Introducing the sys crypto fips module 92-1
Alphabetical list of components 92-1
by-handle 92-2
external-hsm 92-3
key 92-4

93
sys daemon-log-settings

Introducing the sys daemon-log-settings module 93-1
Alphabetical list of components 93-1

clusterd 93-2
csyncd 93-4
icrd 93-6
lind 93-8
mcpd 93-10
tmm 93-12

94
sys disk

Introducing the sys disk module 94-1
Alphabetical list of components 94-1
application-volume 94-2
directory 94-4
logical-disk 94-5

95
sys file

Introducing the sys file module 95-1
Alphabetical list of components 95-1
apache-ssl-cert 95-2
data-group 95-5
external-monitor 95-8
ifile 95-10
rewrite-rule 95-12
ssl-cert 95-14
ssl-crl 95-17
ssl-key 95-19

96
sys fpga

Introducing the sys fpga module 96-1
Alphabetical list of components 96-1
firmware-config 96-2
info 96-4

97
sys icall

Introducing the sys icall module 97-1
Alphabetical list of components 97-1
event 97-2
istats-trigger 97-4
publisher 97-6
script 97-7

98
sys icall handler

Introducing the sys icall handler module 98-1
Alphabetical list of components 98-1
periodic 98-2
perpetual 98-5
triggered 98-8

99
sys ipfix

Introducing the sys ipfix module 99-1
Alphabetical list of components 99-1
destination 99-2
element 99-3
irules 99-6

100
sys log-config

Introducing the sys log-config module 100-1
Alphabetical list of components 100-1
filter 100-2
publisher 100-5

101
sys log-config destination

Introducing the sys log-config destination module 101-1
Alphabetical list of components 101-1
alertd 101-2
arcsight 101-4
ipfix 101-6
local-database 101-9
local-syslog 101-11
remote-high-speed-log 101-13
remote-syslog 101-15
splunk 101-18

102
sys performance

Introducing the sys performance module 102-1
Alphabetical list of components 102-1
all-stats 102-2
connections 102-4
gtm 102-5
ramcache 102-6
system 102-7
throughput 102-8

103
sys raid

Introducing the sys raid module 103-1
Alphabetical list of components 103-1
array 103-2
bay 103-4
disk 103-6

104
sys sflow

Introducing the sys sflow module 104-1
Alphabetical list of components 104-1

receiver 104-2

105
sys sflow data-source

Introducing the sys sflow data-source module 105-1
Alphabetical list of components 105-1
http 105-2
interface 105-3
system 105-4
vlan 105-5

106
sys sflow global-settings

Introducing the sys sflow global-settings module 106-1
Alphabetical list of components 106-1
http 106-2
interface 106-4
system 106-6
vlan 106-8

107
sys software

Introducing the sys software module 107-1
Alphabetical list of components 107-1
block-device-image 107-2
block-device-software-hotfix 107-6
hotfix 107-9
image 107-12
signature 107-15
status 107-17
update 107-19
update-status 107-21
volume 107-23

108
sys url-db

Introducing the sys url-db module 108-1
Alphabetical list of components 108-1
download-result 108-2
download-schedule 108-3
url-category 108-5

109
util

Introducing the util module 109-1
Alphabetical list of components 109-1
ccmode 109-2
dnat 109-3
lsndb 109-5
platform_check 109-8
sipdb 109-9
ssh-keyswap 109-11

test-monitor 109-12
tracepath 109-13
tracepath6 109-14
traceroute 109-15
traceroute6 109-16
vconsole 109-17
zebos 109-18

110
vcmp

Introducing the vcmp module 110-1
Alphabetical list of components 110-1
global 110-2
guest 110-3
vdisk 110-8
virtual-disk 110-9
virtual-disk-template 110-10

111
vcmp health

Introducing the vcmp health module 111-1
Alphabetical list of components 111-1
ha-status 111-2
module-provision 111-3
prompt 111-4
software 111-5

112
wam

Introducing the wam module 112-1
Alphabetical list of components 112-1
ad-policy 112-2
application 112-4
domain-list 112-10
object-type 112-12
policy 112-15
roi-statistics 112-42

113
wam resource

Introducing the wam resource module 113-1
Alphabetical list of components 113-1
concat-set 113-2
domain-list 113-4
url 113-6

114
wom

Introducing the wom module 114-1
Alphabetical list of components 114-1
advertised-route 114-2
deduplication 114-5

diagnose-conn 114-7
endpoint-discovery 114-8
local-endpoint 114-11
remote-endpoint 114-14
remote-route 114-19
server-discovery 114-20
verify-config 114-23

115
wom profile

Introducing the wom profile module 115-1
Alphabetical list of components 115-1
cifs 115-2
isession 115-5
mapi 115-9

Glossary

Index

1

Introducing the Traffic Management Shell

- About the Traffic Management Shell
- Additional command line utilities and tools
- Basic syntax conventions

About the Traffic Management Shell

The BIG-IP® system includes a tool known as the Traffic Management Shell (tmsh) that you can use to configure and manage the system from the command line. Using tmsh, you can configure system features, and set up network elements. You can also configure the BIG-IP system to manage local and global traffic passing through the system, and view statistics and system performance data.

You can use tmsh in conjunction with the Configuration utility, which is the browser-based BIG-IP system and network management tool.

All products in the BIG-IP product family run on the powerful Traffic Management Operating System®, commonly referred to as TMOS®. For an overview of the complete BIG-IP product offering, see the *TMOS® Management Guide for BIG-IP® Systems*.

Additional command line utilities and tools

There are several additional command line utilities and tools that you can use to configure and manage the BIG-IP system:

- The config utility
  You use the config utility to define the IP address, network mask, and gateway for the management (MGMT) port, when you initially set up the BIG-IP system.
- The bigtop utility
  The bigtop utility is a statistical monitoring utility that ships on the BIG-IP system. This utility provides real-time statistical information. You can set a refresh interval and specify a sort order for this statistical information.
- The bigstart command
  With the bigstart command, you can start, stop, restart, and check the status of various daemons, such as snmpd.
- The gencert utility
  You can use the gencert utility to generate a key, a temporary certificate and a certificate signing request file. You then submit the request file to a certificate authority to obtain an SSL certificate.

The industry-standard tools that you can also use to manage the BIG-IP system are:

- The Tools Command Language (Tcl) programming language
  The Tools Command Language (Tcl) programming language is an industry-standard programming language that you can use to create BIG-IP system iRules®. *iRules* are scripts you can write to direct and manipulate the way that the BIG-IP system manages application traffic.
- The OpenSSL utility
  A component of the industry-standard OpenSSL toolkit, the OpenSSL utility is a set of commands that perform various cryptographic functions, such as generating SSL certificates and keys.

Basic syntax conventions

The following table lists basic syntax conventions that apply throughout this guide.

Item in text	Description
( )	Specifies that the syntax inside the parentheses is optional.
...	Specifies that you can type a series of items.
[ ]	Identifies a user-defined parameter in tmsh. For example, if the syntax shows [your name], type in your name, but do not include the brackets.
|	Specifies a choice between options.
[integer]	Specifies a numeric attribute. Unless there is a system assigned default value, the default value is 0 (zero).
[ip address]	Specifies an IPv4 or IPv6 address.
[mac-address]	Specifies a six hexadecimal numbers separated by colons.

Table 1.1 Command line syntax conventions

2

Understanding and Using the Traffic Management Shell

- Understanding the structure of tmsh
- Using tmsh
- Introduction to command syntax

Understanding the structure of tmsh

tmsh is an interactive shell that you use to manage the BIG-IP® system. The structure of tmsh is hierarchical and modular. The highest level is the root module, which contains twelve subordinate modules.

Several modules also contain subordinate modules. All modules and subordinate modules contain components that you configure to manage the BIG-IP system. You can configure a component that resides anywhere in the hierarchy from anywhere else in the hierarchy by using the full path to that component. Alternatively, you can configure a component by navigating to that component directly. After you create a component, you can modify that component in object mode, which is the lowest level of the hierarchy.

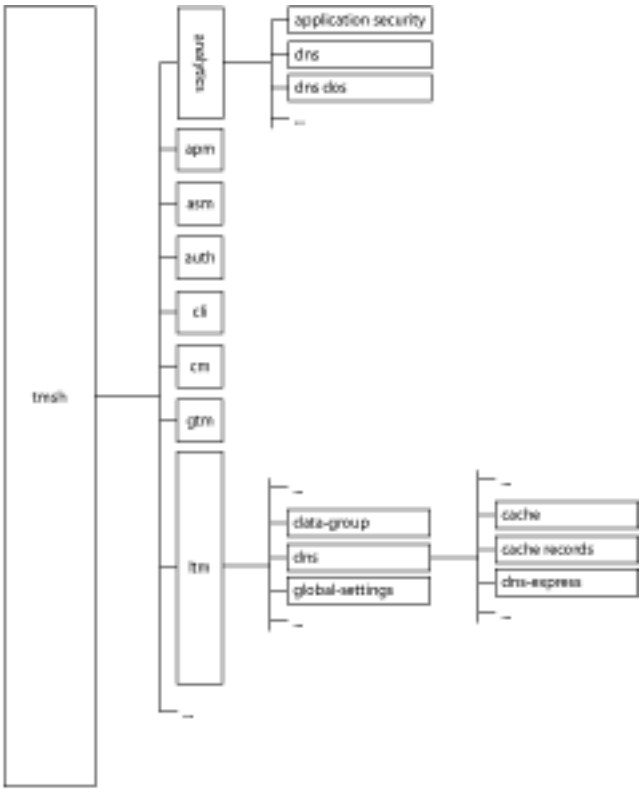

Figure 2.1 The tmsh modular structure

Using tmsh

You must provision a BIG-IP module before you can use tmsh to configure it. The command sequence list sys provision displays the BIG-IP system modules that can be provisioned.

Important

tmsh applies all configuration changes that you make from within tmsh to the running configuration of the system. For tmsh to write the changes to the stored configuration files, you must save the changes using the save sys config command sequence.

You can run tmsh and issue commands in the following ways:

- You can issue a single tmsh command at the BIG-IP system prompt using this syntax:

  ```
  tmsh [command] [module...module] [component] (options)
  ```

  For example, you can display all the properties of all BIG-IP system pools by typing the following command sequence at the BIG-IP system prompt:

  ```
  tmsh show ltm pool all-properties
  ```

- You can open tmsh by typing tmsh at the BIG-IP system prompt. This starts tmsh in interactive shell mode and displays the tmsh prompt: (tmos)#.

Loading and saving the system configuration

The system applies all configuration changes that you make from within tmsh to the running configuration of the system. You can save a portion of the running configuration known as the base configuration. You can also load the base configuration from the stored configuration files.

- To save the base configuration to the stored configuration files, use the following command sequence:

  ```
  save /sys config base
  ```

- To replace the base configuration with the configuration in the stored configuration files, use the following command sequence:

  ```
  load /sys config base
  ```

- To save the entire running configuration to the stored configuration files, use the following command sequence:

  ```
  save /sys config
  ```

- To replace the entire running configuration with the configuration in the stored configuration files using the following command sequence:

  ```
  load /sys config
  ```

Working within the tmsh hierarchy

It is important to understand how to use the command syntax based on where you are in the tmsh hierarchy.

When you are working in the root module, you enter a command sequence using this syntax:

```
[command] [module...module] [component] (options)
```

When you are working in a subordinate module, and you want to configure a component that resides within another module, you enter a command sequence using this syntax:

```
[command] / [module...module] [component] (options)
```

Note that the slash provides the path from one module to another. The first slash can optionally have space after it; "/ ltm" is equivalent to "/ltm."

As you navigate within tmsh, the prompt contains a visual cue to your location within the hierarchy.

You can navigate to a module, a component within a module, or a specific component (object mode). The following list provides examples of how the tmsh prompt changes as you navigate through the hierarchy. From the root module prompt:

- To navigate to the ltm module, type: ltm
  The ltm module prompt displays: (tmos.ltm)#
- To navigate to the ltm pool component, type: ltm pool
  The ltm pool component prompt displays: (tmos.ltm.pool)#
- To navigate to pool1, type: modify ltm pool pool1
  The pool1 object prompt displays: (tmos.ltm.pool.pool1)#

◆ Note

You can navigate only to an object that already exists, and you must use the modify command to navigate to that object.

◆ Tip

You can change the information that displays in the tmsh prompt, but the prompt always includes your location in the hierarchy and ends with a pound sign (#). For information about customizing the prompt, see the documentation for preference, on page 43-6.

Working within a module

From the root module, you can navigate to another module by entering the name of the module at the prompt. tmsh opens the module, and displays the prompt: (tmos.module)#

For example, from the root module, to navigate to the gtm module, type:

```
gtm
```

The prompt now indicates that the current location in the hierarchy is the gtm module.

Within a module, you can type a command sequence using this syntax:

```
[command] [component] (options)
```

For example, you can display all the properties of all Global Traffic Manager™ pools by entering the following command sequence at the gtm module prompt:

```
list pool all-properties
```

Additionally, from a module, you can manage a component in a different module using this syntax:

```
[command] / [module...module] [component] (options)
```

For example, from the gtm module, you can show all of the properties of the VLANs on your network by entering the following command sequence at the gtm module prompt:

```
list / net vlan all-properties
```

Working within a component

From a tmsh module, you can navigate to a component by entering the name of the component at the prompt. tmsh displays the component prompt: (tmos.module.component)#

For example, from the gtm module, to navigate to the gtm pool module, type:

```
pool
```

The prompt now indicates that the current location in the hierarchy is the gtm pool component.

Within the component, you can type a command sequence using this syntax:

```
[command] (options)
```

For example, you can display all of the properties of all of the Local Traffic Manager™ pools by entering the following command sequence at the ltm pool component prompt:

```
list all-properties
```

From within a component, you can also manage a component in a different module using this syntax:

```
[command] / [module...module] [component] (options)
```

Note that you can manage a component from anywhere within the tmsh hierarchy by using the full path to the component.

For example, from the gtm pool component, you can show all of the properties of the VLANs on your network by entering the following command sequence at the prompt:

```
list / net vlan all-properties
```

Working in object mode

From a tmsh component, you can navigate to a specific object of that type, by entering the modify command followed by the name of the component at the prompt. tmsh opens the component and displays the prompt: (tmos.module.component.object_name)#

For example, from the gtm pool module, to navigate to the Global Traffic Manager pool, named pool1, type:

```
modify pool1
```

The prompt now indicates that the current location in the hierarchy is the gtm pool pool1 object.

The Properties list contains the available properties of the current object.

For example, to navigate to the Global Traffic Manager pool named pool1 type the following command sequence:

```
modify gtm pool pool1
```

tmsh displays this prompt: (tmos.gtm.pool.pool1)#

In the object mode, you can type a command sequence using this syntax:

```
[command] (options)
```

For example, you can display all of the properties of gtm pool1 by entering the following command sequence at the gtm pool1 object prompt:

```
list all-properties
```

From within an object, you can also manage a component in a different module using this syntax:

```
[command] / [module...module] [component] (options)
```

For example, from within the gtm pool pool1 object, you can display all of the properties of the Local Traffic Manager™ pool named my_ pool by entering the following command sequence at the gtm pool pool1 object prompt:

```
list / ltm pool pool1 all-properties
```

Leaving object mode, component mode, a module, or tmsh

Table 2.1 describes the commands you use to navigate out of a mode or a module, and eventually close tmsh and return to the BIG-IP system prompt.

Command	Action
/	From any level of the tmsh hierarchy, returns you to the root module.
exit	From within object mode, returns you to the component within which the object resides. From within a component, returns you to the module within which the component resides. From within a module, returns you to the parent module.
quit	From within a module, closes tmsh.

Table 2.1 Commands for navigating out of a mode or module, and for closing tmsh

Using the scripting feature

You can use the tmsh script component to build Tcl scripts to automate and customize management of the BIG-IP system. The tmsh scripting feature is a small API that provides structured programmatic access to all system configuration, status, and statistics. The API mirrors the interactive command line syntax. The structured access of the API eliminates the need to screen scrape output.

Using the tmsh scripting feature, you can write scripts that perform the following:

- Accept parameters from the command line
- Provide command completion and context-sensitive help
- Handle the management of complex system configurations with simple form-based input
- Run in their own execution environment separate from the shell from which they were started

This feature also gives you the ability to perform the following:

- Build reusable script libraries and include them in other scripts using the #include directive
- Use transactional semantics
- Combine command aliases with scripts, allowing you to extend tmsh to build commands that are customized to your environment

Checking the Current tmsh Version

Each release of tmsh has a unique tree of modules and components, so if a tmsh script functions with one version, it may not function with another. To see the current version of tmsh, use the following command sequence:

```
show cli version
cli version {
    active 11.5.0
    latest 11.5.0
    supported { 11.5.0 }
}
```

This identifies the currently-active tmsh version as well as all the versions supported on this system.

Changing the tmsh to a Former Version

For a script that supports an older version of tmsh, you can use the **modify cli version** command to set the active tmsh version:

```
modify cli version active new-version
```

This changes the tree of available modules and components to be compatible with the tmsh version that you choose. The tmsh interface reverts entirely to the former version. If you place this command at the top of a script that was built for the given version, the script functions the same way it did on earlier releases of the software.

Software Release 11.5.0 is the first release to support tmsh version control. We recommend setting the version to 11.5.0 at the top of your 11.5.0 tmsh scripts, to guard against the script breaking in a future version of tmsh.

Using the command completion feature

At any point while typing or editing a command in tmsh, you can press the Tab key. tmsh either completes the current or next word, or displays possible completions for the current or next word.

The command completion feature reduces the amount of typing that is required to run commands. When you press the Tab key, the system automatically completes the current command-line element to as many unique characters as possible. If there is more than one possible completion the list of possible completions displays. Command completion also completes configuration object identifiers.

For example, if the command has only one option, tmsh fills in the remainder of the word with that option and a trailing space. If the command has more than one option, tmsh completes the current word with the longest possible match, while also displaying the other possible matches. If tmsh displays nothing after you press the Tab key, no options exist to complete the word.

If you move the cursor anywhere on the command line and press the Tab key, tmsh completes what is to the left of the cursor. For example, tmsh completes sho[Tab] pool as show pool.

Using glob matching with the command completion feature

tmsh uses glob matching to complete object identifiers. *glob matching* checks for the presence of the constituents of a given pattern. This means that if you partially type an object identifier, such as the IP address of a node, tmsh completes the command by offering all IP addresses that contain the partial address you entered.

For example, tmsh returns addresses that match 10.1.1* when you type the following command sequence:

```
show node 10.1.1[Tab]
```

Likewise, tmsh returns addresses that match 10*22*, when you type the following command sequence:

```
show node 10*22[Tab]
```

Understanding the behavior of the command completion feature

There are several behaviors to be aware of when using the command completion feature. When you press the Tab key, the components that display in the Configuration Items list are determined by your permissions and the action you are taking. The following rules apply:

- When you configure a component that is not a child component, the Configuration Items list contains the existing components of the type that you are configuring that you have permission to view.

  For example, tmsh displays all virtual servers that you have permission to view in the Configuration Items list when you configure a virtual server using the following syntax:

  ```
  [create | delete | modify] virtual [Tab]
  ```

- When you configure a child component, (for example, when you add a pool member to a pool), the Configuration Items list contains the existing components of the type that you are configuring based on the following rules:

  - When you add a child component to its parent, the list contains only the components of that type that you have permission to view that are not yet associated with the parent component. For example, the list contains all of the virtual servers that you have permission to view that are not yet associated with poolA when you add members to poolA using the following syntax:

    ```
    modify pool poolA members add { [Tab]
    ```

  - When you replace all of the child components that are associated with a parent component, the list contains all of the components of that type that you have permission to view. For example, the list contains all of the virtual servers that you have permission to view when you replace all of the members of poolA using the following syntax:

    ```
    modify pool poolA members replace-all-with { [Tab]
    ```

- When you delete or modify the child components that are associated with a parent component, the list contains only the components of that type that are already associated with the parent. For example, the list contains all of the virtual servers that are currently a member of poolA when you delete the members of poolA using the following syntax:

  ```
  modify pool poolA members delete { [Tab]
  ```

- When you configure a component, the Properties list only contains properties that you can use with other already configured properties of that component.

  The command route is a good example. If you specify a pool for the route, then the interface, gateway, and blackhole options are no longer valid, so they do not appear in the list.

Tip

At the BIG-IP system prompt, tmsh displays possible completions for a command, only if you type the tmsh command followed by:
Ctrl + V Ctrl + T Enter

Using the help feature

tmsh includes man pages for each of the commands and components that are available within tmsh. You access the man pages using the following command syntax:

```
help [ [command] | [full path to component]
```

For example, to access the man page for the vlan component from the root module, use the following command sequence:

```
help / net vlancl
```

You can also search the man pages for information on a specific term or topic. To do this, you use the following command syntax:

```
help search [term or topic]
```

You can perform a help search from within any module in the tmsh hierarchy. For example, to find the man pages that contain a reference to VLANs, use the following command sequence:

```
help search vlan
```

Additionally, you can display a list of topics that are available in a module using the following command sequence:

```
help [full path to module]
```

For example, to display the topics that are available in the current module, use this command: help. To display the topics that are available in the net module, use the following command sequence: help / net.

Using the context-sensitive help feature

tmsh includes a context-sensitive help feature that provides help as you type commands. At any time, you can type a question mark (?) on the command line, and tmsh returns information to assist you in completing the command. Based on when you type the question mark, you get the following results:

- When you type a question mark immediately following any portion of a command, tmsh returns possible completions for the command, but does not complete the command as the command completion feature does.
- When you type a space before the question mark, tmsh returns descriptive text that explains the commands, components, or properties that you can configure.
- When you type a question mark in the middle of a command, tmsh returns help on the command to the left of the cursor.

◆ Note

To use a question mark in a glob or regular expression, you must escape the question mark using quotation marks, apostrophes, or a backslash.

Additionally, you can request context-sensitive help for the last command in a series of commands. For more information, see *Entering multiple commands*, on page 2-10.

Interrupting a command

You can cancel a command that you issued by typing Ctrl + C one or more times.

Entering multiple commands

You can enter multiple commands on the command line by separating the commands with semi-colons (;). For example, to display the properties of the self IP addresses and VLANs of the system, use the following command sequence:

```
list / net self ; list / net vlan
```

When you enter multiple commands in this way, all of the commands are added to the command glob in a single line item, regardless of whether any of the commands were successful. However, if one of the commands that you enter fails to parse, tmsh does not run the remaining commands you entered. tmsh audits commands as the commands run; therefore, if a command fails to parse, tmsh does not audit the remaining commands.

You can also specify multiple commands in a command alias by separating the commands with semi-colons. For example, to create an alias that displays the properties of the VLANs and VLAN groups on the system, use the following command sequence:

```
create / cli alias vlans command "list / net vlan ; list / net
vlan-group"
```

Additionally, you can request context-sensitive help and use the command completion feature on the last command in a series of commands. For example, to display help for the vlan-group component, use the following command sequence:

```
list / net vlan ; list / net vlan-group ?
```

Using the command glob feature

tmsh saves each command that you enter in the command glob file. The date and time the command was issued displays before the command in this format: [Month day hh:mm:ss]. You can disable this feature.

To change whether the date and time display in the glob file

1. Log on to tmsh and navigate to the cli preference module.
2. To disable the display of the date and time in the glob file, type:

   ```
   modify glob-date-time disabled
   ```
3. To enable the display of the date and time in the glob file, type:

   ```
   modify glob-date-time enabled
   ```

The command glob persists when you log off of the system. The next time you log on to the system, you can search for, display, and then edit, the tmsh commands that you entered in previous sessions. The command glob persists even through a restart of the BIG-IP system.

There are two limits that you can set for the command glob: the number of commands that tmsh saves in the command glob file, and the number of commands that you can view or search from the command line.

- You use the set cli preference glob-file-size command to set the maximum number of commands that you want tmsh to save in the command glob file.

  The default is 10,000 commands. The maximum number of commands that the file can contain is 100,000 commands. If you do not want to use the command glob feature, set the maximum number of commands to 0 (zero). This means that tmsh does not save any commands in the glob file.
- You use the set cli preference glob-size command to set the number of commands that you want to be able to view or search from the command line.

  The default is 500 commands. The maximum number of commands that you can view or search is 10,000 commands. When you set the glob-size option to (0) zero, tmsh does not add commands to the in-memory list of commands, but does continue to write commands to the command glob file.

Note: After you change the value of the glob-size option, tmsh might renumber the commands; however, the commands remain in the same order.

◆Tip

tmsh does not save commands in the command glob file that end in a question mark (?) or begin with an exclamation point (!). Likewise, these types of commands do not appear in the command glob list.

To display the commands in the tmsh glob list

1. Log on to tmsh.
2. Enter an exclamation point (!).
   The command glob list displays the previously used commands in the reverse order of use.
3. After you locate the command that you want to use again, type:

   ```
   ! [numeric ID]
   ```

   For example, to run the command with a numeric ID of 32, type:

   ```
   !32
   ```

◆Note

Each command in the glob list is identified by a numeric ID. The larger the ID, the more recently the command was issued relative to other commands.

To search for and run a command in the tmsh glob list using a partial string

1. Log on to tmsh.
   The tmsh prompt displays.
2. To run the most recent command in the glob list that begins with the specified string, type the following command:

   ```
   ![string]
   ```

   tmsh locates the command in the glob list and runs it.

   For example, from the cli module, to run the most recent command that you used to set the preferences for the command line, type: `!set preference`.

When you are logged on to tmsh, you can use the glob list to run the previous command, even if it was run in the previous tmsh session.

To run the previous command

1. Issue commands to configure the system.
   tmsh runs the commands you issue.
2. Type the following command:

   ```
   !!
   ```

The previous command runs.

When you are logged on to tmsh, you can use pager's search feature to locate a tmsh command by date/time stamp.

To search for a command using the pager's search feature

1. Log on to tmsh.
2. Type one of the following commands:

   ```
   show glob
   ```

   or

   ```
   !
   ```

3. Use the pager's search feature to find a specific date and time.

When you are logged on to tmsh, you can pipe the output of the glob file to the grep utility to search for a command by the date/time stamp.

To search for a command using the grep utility

1. Log on to tmsh.
2. Type the following command:

   ```
   show glob | grep "[hh:mm:ss]"
   ```

Using the tmsh keyboard map feature

You can use the default keyboard map to search the command glob list for a specified command. For example, to search for the previous command that contains a specified string, type the following command:

```
[string] Alt-P
```

You must press Enter to run the command.

The following table describes the default keyboard map for tmsh. The key sequences are not case-sensitive.

Key Sequence	Action
Ctrl + A	Moves the cursor to the beginning of the line.
Ctrl + B	Moves the cursor to the left one character.
Ctrl + C	Cancels the current command.
Ctrl + D	Deletes the character under the cursor, or when the command line is empty, exits tmsh.
Ctrl + E	Moves the cursor to the end of the line.
Ctrl + F	Moves the cursor to the right one character.

Table 2.2 Default keyboard map for tmsh

Key Sequence	Action
Ctrl + G	Clears all characters from the command line.
Ctrl + H	Deletes the previous character.
Ctrl + J	Enters a new line and runs the current command.
Ctrl + K	Deletes all characters from the cursor to the end of the line.
Ctrl + L	Clears the screen, repositions the prompt at the upper left, and leaves the current command intact.
Ctrl + M	Enters a new line and runs the current command.
Ctrl + N	Displays the next item in the command glob.
Ctrl + P	Displays the previous item in the command glob.
Ctrl + Q	Resumes input.
Ctrl + R	Clears the screen, repositions the prompt at upper left, and leaves the current command intact.
Ctrl + S	Suspends input.
Ctrl + T	Transposes the character under the cursor with the character to the left of the cursor.
Ctrl + U	Deletes all characters before the cursor.
Ctrl + W	Deletes the word before the cursor.
Esc + B	Moves the cursor one word to the left.
Esc + D	Deletes all characters from the cursor to the end of the current or next word.
Esc + F	Moves the cursor one word to the right.
Esc + L	Changes the word to the right and the word under the cursor to lowercase.
Esc + N	Searches command glob search for the next item.
Esc + P	Searches command glob search for the previous item.
Esc + U	Changes the word to the right and the word under the cursor to uppercase.
Esc + Backspace	Deletes the word to the left of the cursor.
Backspace	Deletes the character to the left of the cursor.
Delete	Deletes the character to the left of the cursor.

Table 2.2 Default keyboard map for tmsh (Continued)

Key Sequence	Action
Up Arrow	Scrolls back through the command glob.
Down Arrow	Scrolls forward through the command glob.

Table 2.2 Default keyboard map for tmsh (Continued)

Using the command audit feature

The BIG-IP system contains a read-only audit file named /var/log/audit. tmsh writes an entry in the audit file for each tmsh command that runs, providing a historical log of issued commands. Only users with the role of Administrator or Resource-Administrator can view the audit logs.

You can change whether tmsh audits commands using the following syntax:

```
modify / cli global-settings audit [enabled | disabled]
```

◆ Note

If tmsh cannot connect to the mcpd daemon, tmsh audits all commands until the connection is re-established.

Understanding the audit log entries

The audit file contains entries with the format shown in Figure 2.2.

```
01420002:5: AUDIT - pid=number user=user_id query_partitions=p1,p2,…,pn
update_partition=partition_name module=(tmos.module…)# status=[success/fail]
cmd_data=command that was issued
```

Figure 2.2 Audit file entry format

Table 2.3 defines each portion of an audit entry in the order of appearance in the entry.

Audit Entry	Definition
01420002:5: AUDIT	Identifies the entry as a tmsh command.
pid=number	Specifies the process ID of the tmsh instance that generated the entry.
user=user_id	Identifies, by user ID, the user who issued the tmsh command. For commands run by the system, this portion of the entry is empty, for example: user=" ".
query_partitions=	Identifies the administrative partitions, in a comma-separated list, that the user can query. For more information about setting the administrative partitions that a user can query, see *admin-partitions*, on page 43-2.

Table 2.3 Audit entries defined

Audit Entry	Definition
update_partition=	Identifies the administrative partitions that the user can update. For more information about setting the administrative partitions that a user can update, see t*admin-partitions*, on page 43-2.
module=	Identifies the tmsh module within which the user issued the command.
status	Indicates whether the command was run successfully. The possible values are: • Command OK Indicates that the command was successful. • [error syntax] Displays the same error that the system displayed when the command failed. Note that when you use the edit command, and it fails, the audit log contains each line of the file that you attempted to run with the error displayed.
cmd_data=	Indicates the command sequence that the user entered. Note that when the edit command runs successfully, the audit file contains each line of the file that was submitted as a separate entry. For more information about the command edit, see GTM *rule*, on page 46-44.

Table 2.3 Audit entries defined (Continued)

Viewing historical logs

When you view an audit log from the sys module, you can use the lines or range options to reduce the number of log entries that display.

To view historical logs

1. Log on to tmsh.
   The tmsh prompt displays.
2. Type the following command sequence:

   ```
   show / sys log audit lines 5
   ```

   The first five lines in the audit log display.

Using the command aliases feature

You can create command aliases to use as short cuts within tmsh. For example, if you perform specific operations on a regular basis, or if you configure the system using long commands, you can create a command alias to save you some typing.

You can issue a command alias from within any tmsh module. For example, if you create an alias named show to display all of the components in the ltm module, when you type show in the cli module, tmsh displays only the ltm module components. This example illustrates that the command alias you created takes precedence over the system default show command, which normally displays the components of the module within which you issue the command.

WARNING

Aliases that you create take precedence over system commands. Additionally, an alias with the same name as a tmsh module causes the module to be hidden from the command completion feature.

Creating command aliases

A command alias consists of a name and a command sequence that runs when you use the name of the command alias on the command line. When you create a command alias, the name of the command alias:

- Is not case-sensitive
- Cannot be create or delete
- Cannot contain spaces, tabs, exclamation points, or question marks

The following rules apply to the command sequence for which you are creating a command alias.

- The command cannot be empty.
- You can use multiple command sequences, separated by semi-colons.

- You can use another alias as the first argument in the command sequence.
- tmsh does not verify validity of the command sequence until you issue the command alias.
- When you include an exclamation point in the command sequence, the exclamation point does not invoke the command glob.
- If you include spaces in the command sequence, then you must use quotation marks around the command sequence.

Using command aliases

When you use a command alias on the command line, the following rules apply.

- When you use a command alias within a command, you must use the alias at the beginning of the command sequence.
- When you use the command completion or context-sensitive help feature with a command alias, tmsh responds as if you had entered the command sequence that the command alias references.
- Command aliases display in all command completion lists, regardless of whether the command itself is valid within the current module.
- The name of the command alias displays in the command glob list.
- The command, for which you created the alias, not the name of the command alias, displays in error messages related to usage of the alias.

Setting the tmsh preference show-aliases

You can configure tmsh to include command aliases in the list of commands in the Commands section on the command line when you use the command completion and context-sensitive help features.

To set the tmsh preference show-aliases

1. Log on to tmsh.
2. Type the following command:

   ```
   cli
   ```

3. Type the following command sequence:

   ```
   set preference show-aliases enabled
   ```

   When you type a question mark (?) on the command line or use the command completion feature, tmsh now displays command aliases in the Commands section on the command line.

Using the wildcard search feature

tmsh supports regular expression (RE) and glob-based wildcard search methods. For more information about these programs, access the man page for each program using the following tmsh commands:

- help regex
- help glob

Using the statistics feature

You can use tmsh to display statistics, including historical performance statistics. You can select the format in which these statistics display, as well as reset the statistics for some of the tmsh components. To determine if statistics are available for a specific component, see the specific component in one of the following chapters.

Configuring preferences for and viewing statistics from tmsh

You can view statistics for many of the tmsh components using the show command. You can specify the units in which you want tmsh to display statistics. You do this using the following command syntax:

```
set / cli preference stat-units [default | kil | meg | gig |
raw]
```

For example, to set tmsh to display statistics in parts per million, use the following command sequence:

```
set / cli preference stat-units meg
```

While you are working in tmsh, you can override the stat-units setting to display statistics for a specific component in a different unit. For example, to display the statistics for the ltm pools in gigabits, use the following command sequence:

```
show / ltm pool gig
```

Table 2.4 describes the units in which tmsh can display statistics.

Option	Description
default	Displays data in the simplest units. For example, if the data is 1,200,001, tmsh displays 1.20M; however, if the data is 1,200, tmsh displays 1.2K. This is the default value for system statistics.
gig	Displays data in parts per billion.
kil	Displays data in parts per thousand.

Table 2.4 Unit options for statistics described

Option	Description
meg	Displays data in parts per million.
raw	Displays raw data.

Table 2.4 Unit options for statistics described (Continued)

For some tmsh components, you can choose the level of statistics that you want to view. Table 2.5, on page 2-21, contains a description of the options you can use to display statistics, depending upon the information that you want to view. Note that all levels are not available for all components. To determine which of these options is available for a specific component, refer to the man page for the component, use the command completion feature, or see Chapter 3, *Global Commands*.

To display the statistics for a specific component at a specific level, use the following command syntax:

```
show / [module...module] [component] [detail | global |
historical]
```

For example, use the following command sequence when you want to view detailed pool statistics for Local Traffic Manager pools:

```
show / ltm pool detail
```

tmsh also provides a historical view of system performance. You can use the historical option, shown in Table 2.5, on page 2-21, to display historical performance data. This option displays data that is equivalent to the performance graphs in the Configuration utility. For more information, see *Collecting performance data* in the *TMOS® Management Guide for BIG-IP® Systems*.

For example, to display statistics about current connections, and for connections that have occurred within the last 3 hours, 24 hours, 7 days, and 30 days, use the following command sequence:

```
show / sys performance connections historical
```

The components for which you can view historical data are in the system performance module. They include connections, gtm, ramcache, system, and throughput.

Show Command Option Used	Statistics that display	Syntax of show command
detail	Statistics for all of the components of the specified type, and the components with which these components are associated.	`show / [module...module] [component] detail`
	Statistics for the specified component, and the components with which the specified component is associated.	`show / [module...module] [component] [component_name] detail`
global	Roll-up statistics for the component, and all related components.	`show / [module...module] [component] global`
	Roll-up statistics for the specified component, and all related components.	`show / [module...module] [component] [component_name] global`
historical	Historical system performance statistics.	`show / system performance [component] historical`

Table 2.5 Levels in which you can display statistics in tmsh

◆Tip

You can also view statistics from the BIG-IP system prompt, using the following command syntax: tmsh show / [module...module] [component] \ [detail | global | historical] [default | kil | meg | gig | raw]

Resetting statistics

When you are evaluating the performance of your system, you might want to reset the statistics for a component. You can do that in one of two ways:

- You can reset the statistics for a type of component using this syntax:

```
reset-stats / [module...module] [component]
```

- You can reset the statistics for a specific component using this syntax:

```
reset-stats / [module...module] [component] [component_name]
```

◆ Note

After you reset statistics, when you run the show command, you might see a value of nan. This stands for not a number, which indicates that no data is currently available. Wait a few moments and run the show command again, and in most cases the nan value will be replaced by an integer value.

Using grep functionality in tmsh to filter output

grep is a command line search utility. For more information about grep, see the man page using the tmsh command help grep.

To use the output of a tmsh command as input to the grep utility, use this syntax:

```
[command] | grep [grep options]
```

tmsh supports the grep utility options shown in Table 2.6.

Supported option	Usage
-A, -B, -C, -m	These options require a numeric argument between 0 and 4294967295.
-c, -E, -G, -i, -n, -o, -P, -v, -w, -x	These options do not accept arguments. Instead, the grep utility treats arguments for these options as either another option or a search pattern.
-e	This option requires one argument, a search pattern.
-[unsupported option]	Unsupported options preceded by a hyphen result in syntax errors.
[argument]	tmsh treats any argument that is not preceded by a supported option, and does not begin with a hyphen, as a search pattern preceded by -e. For example, if you enter show pool | grep 10.2.3.4 within the ltm module, tmsh runs show pool | grep -e 10.2.3.4.

Table 2.6 grep utility options supported in tmsh

Creating batch mode transactions

You can issue a set of commands in a batch, and tmsh processes the commands as a single transaction. You enter batch mode by using the transaction component within the cli module.

When you run a set of commands in batch mode, tmsh does one of two things:

- Successfully runs all of the commands in the transaction.
- Does not commit any of the commands in the transaction, if the syntax of any of the commands does not pass the syntax check. In other words, tmsh does not partially commit a transaction.

To create a batch mode transaction

1. Log on to tmsh.
2. Type the following command sequence:

   ```
   create /cli transaction
   ```

   The tmsh batch mode prompt displays: [batch mode] (tmos)#.
3. Enter a command using the full path to the command.
   tmsh parses the command, and if the command passes syntax checks, tmsh indicates that the command has been added to the transaction.

To view the commands in the transaction

At the tmsh batch mode prompt, type:

```
list transaction
```

tmsh displays the commands in the transaction by numeric ID.

To delete a command from the transaction

At the tmsh batch mode prompt, type:

```
modify transaction delete [numeric ID]
```

tmsh deletes the command that you specify with a numeric ID. Note that the system might renumber the commands in the transaction.

To replace a command in the transaction

At the tmsh batch mode prompt, type:

```
modify transaction replace [numeric ID] [command sequence]
```

tmsh checks the syntax of the new command that you specify with a numeric ID, replaces the existing command identified by the numeric ID with the new command, and indicates that the transaction was updated successfully.

To insert a command in the transaction

At the tmsh batch mode prompt, type:

```
modify transaction insert [numeric ID] [command sequence]
```

tmsh checks the syntax of the new command that you specify to insert before a command identified by a numeric ID, renumbers the existing commands identified, and indicates that the transaction was updated successfully.

To submit the transaction

At the tmsh batch mode prompt, type:

```
submit transaction
```

tmsh runs the transaction. Note that if the transaction fails, tmsh remains in batch mode, and you can update the transaction, and then resubmit it.

To cancel the transaction

At the tmsh batch mode prompt, type:

```
delete transaction
```

tmsh deletes all the commands in the transaction and returns you to the tmsh prompt.

Controlling tmsh

tmsh includes a set of commands that you can use to change the behavior of tmsh, and to configure the BIG-IP system. For more information about the tmsh commands, see Chapter 3, *Global Commands*, or use the help command within tmsh.

Changing the behavior of tmsh

The options that you can use to change the behavior of tmsh are described in Table 2.7.

Options	Action
-a	tmsh does not write commands to the command glob file. For more information about the command glob file, see *Using the command glob feature*, on page 2-11. Note that if auditing is enabled, tmsh continues to write commands to the audit log. For more information, see *Using the command audit feature*, on page 2-15. This option is useful when writing scripts, because it stops the scripts from filling up the command glob file. This option applies to the non-interactive mode only.
-c	Disables video highlighting in tmsh.
-d [ip address | hostname]	Connects to the specified blade in a clustered system.
-h	Displays options you can use when accessing tmsh from the system shell.

Table 2.7 Commands that alter the behavior of tmsh

Options	Action
-m	Generates a tmsh debug log file name tmsh.out in the current directory. Note that when you run a tmsh script, the shell generates a debug log file for the script named tmsh.out.[script name]. Using this option causes tmsh to run significantly slower.
-q	Prevents tmsh from responding to user actions with questions. This option is useful when writing non-interactive shell scripts from the system shell.

Table 2.7 Commands that alter the behavior of tmsh (Continued)

Using special characters in tmsh

You can use special characters when running tmsh commands. Table 2.8 lists these special characters, describes how to use them, and provides examples of their usage.

Character	Usage	Examples
`" "`	Use quotation marks around strings that contain a space, a backslash (\) that is not being used to escape another character, or an apostrophe (’).	`create partition A description "Admin’s partition"`
`’ ’`	Use apostrophes around arguments, a string with a space, a string with a backslash (\), or a string with a double-quote (").	`create partition A description ’Admins partition’`

`\`	Use a backslash to escape the following: quotation marks (" "), another backslash (\), an asterisk (*), a question mark (?), a left bracket ([), or a space.
	Inside a pair of apostrophes or double quotes, you do not need to escape the backslash (\).
		`list gtm wideip "\*siterequest.com"`
		`list gtm wideip "\*site\?.com"`
		`list gtm wideip \\*siterequest.com`
		`list gtm wideip \\*site\\?.com`

`*`	When escaping glob and regex special characters, use an asterisk (not between brackets) in a search string to match any string including an empty string. Use a backslash (\) to escape an asterisk.	`list gtm wideip "\*siterequest.com"`

Table 2.8 Special character usage in tmsh

Character	Usage	Examples
?	When escaping glob and regex special characters, use a question mark (not between brackets) in a search string to match a single character. Use a backslash (\) to escape a question mark.	`list gtm wideip "\*site\?.com"`
[]	When escaping glob and regex special characters, use brackets to enclose any characters that you want to include in a search string to match a single character. Use a backslash to escape square brackets.	`list gtm datacenter \[site]`
space	You must escape the space character or put quotation marks around it.	`create gtm pool my\ http\ pool` `create gtm pool "my http pool"`
|	Use the vertical bar to filter output from the commands show or list.	`show ltm pool | grep 10.2.3.4` `list ltm pool | grep 10.2.3.4`

Table 2.8 Special character usage in tmsh (Continued)

Introduction to command syntax

The remainder of this guide contains the command syntax for tmsh global commands and for configuring the tmsh components. You can also find information about tmsh command syntax in the man pages. You can display a tmsh man page from the tmsh prompt, by entering help followed by the full path to the component name. For example, to display the man page for the Global Traffic Manager pool component from the root module, use the following command sequence:

```
help / ltm pool
```

3

Global Commands

- Introducing global commands
- Alphabetical list of global commands

Introducing global commands

You can use the tmsh global commands within any tmsh module. For more information about the tmsh hierarchical structure, see Chapter 2, *Understanding and Using the Traffic Management Shell*.

Alphabetical list of global commands

The remainder of this chapter lists the tmsh global commands.

cd

Change the current working folder.

Syntax

Use the command **cd** to change the current working folder.

```
cd [folder name]
cd /[folder name]
```

Description

The command **cd** [folder name] changes the current working folder to allow the user navigation around the folder system (see **sys folder**). The command **pwd** displays the current working directory.

The current working folder may be listed in the tmos command prompt while in tmsh interactive mode (see **cli preference**).

Folder names are separated by a forward slash **/**.

There are two built-in folders:

/ is the root folder

/Common is the default folder for creating new configurations objects.

Additionally, the following directory entries:

. is the current folder

.. is the parent folder

Examples

cd /Common

Change the current working folder to /Common.

cd resources

Change the current working folder to resources. In this example the resources
folder is relative to the current working folder. As an example, if the current working folder was /Common, the new working folder will be /Common/resources.

cd resources/profiles/udp

Multiple folders may be specified. Tab complete assists filling the command line
with folder names.

cd /

Make the current working folder the root folder.

cd ../Alpha

Change the working directory by first going to the parent, and then switch to the sub-folder Alpha.

See Also

help, *pwd*, *folder*, *tmsh*

cp

Creates a copy of a TMOS™ configuration object.

Syntax

Use the command **cp** within a **tmsh** module to create a copy of the component that resides in that module. To create a copy component that resides in another module, use the full path to the component.

```
cp [component] [source] [destination]
cp / [module...module] [component] [source] [destination]
```

Description

You must provide a unique name for each component destination of the copy operation.

Examples

cp template mytemplate newtemplate

From within the **sys application** module, creates a new Application Template named **newtemplate** with the same properties as **mytemplate** .

cp / cli script my_script1 my_script2

From within the **sys application** module, copies the **my_script1** script to **my_script2** within the **cli** module.

Options

- **component**
  Specifies the type of the component that you want to copy.
- **module**
  Specifies the module within which the component that you want to copy resides.
- **source**
  Specifies the component to be copied.
- **destination**
  Specifies a unique name for the component that will be created as part of the copy.

See Also

tmsh

create

Creates a TMOS™ configuration component.

Syntax

Use the command **create** within a **tmsh** module to create a component that resides in that module. To create a component that resides in another module, use the full path to the component.

```
create [component] [name] [property [value]...]
create / [module...module] [component] [name] [property [value]...]
```

Description

You must provide a unique name for each component that you create.

Examples

create pool pool1

From within the **gtm** module, creates a Global Traffic Manager pool named **pool1**.

create / ltm pool my_pool

From within the **gtm** module, creates a Local Traffic Manager pool named **my_pool**.

Options

- **component**
  Specifies the type of the component that you want to create.
- **module**
  Specifies the module within which the component that you want to create resides.
- **name**
  Specifies a unique name for the component.
- **property [value]...**
  Specifies properties for the component and their values.

See Also

tmsh

delete

Deletes a **tmsh** component.

Syntax

Use the command **delete** within a **tmsh** module to delete a component that resides in that module. To delete a component that resides in another module, use the full path to the component.

```
delete [component] [name]
delete / [module...module] [component] [name]
```

Description

You must provide the name of the component that you want to delete.

Examples

delete pool pool1

From within the **gtm** module, deletes the Global Traffic Manager pool named **pool1**.

delete / ltm pool my_pool

From within the **gtm** module, deletes the Local Traffic Manager pool named **my_pool**.

Options

- **component**
  Specifies the type of the component that you want to delete.
- **module**
  Specifies the module within which the component that you want to delete resides.
- **name**
  Specifies the name of the component that you want to delete. **All** may be used as an identifier for most component types.

- **recursive**
  Deletes all items in the current folder and all sub-folders that match the **module**, **component** and the **name** specified. **all** may be used as the **name** identifier with this command.

◆ Note

*When using **recursive** and **all** together, you will be prompted to verify this action. If you wish to disable this prompt, you may run **tmsh** using the **-q** command-line option. This is very useful when writing scripts that use this command.*

See Also

tmsh

edit

Opens the specified components in an editor.

Modules

All **tmsh** modules.

Syntax

Use the command **edit** to create components or modify the configuration of components using a text editor. To edit a component that resides in another module, use the full path to the component.

```
edit [component] [name ... name | all]
edit / [module...module] [component] [name ... name | all]
```

Description

You can use the command **edit** to create or modify components in the **auth**, **cli**, **gtm**, **ltm**, **net**, **sys** and **wom** modules, and iRules®.

If you are assigned the role of **Administrator**, when you use the command **edit**, the system starts the **vi** editor. If you are assigned any other role, the system starts the **pico/nano** editor.

The system saves, in a temporary directory, the text file, named **data**, that you are editing. When you save the file and close the editor, the system checks for errors, and then prompts you with an opportunity to continue editing and resolve any errors.

When you edit an existing component that can have associations, such as a Global Traffic Manager wide IP that can have pool member associations. but the component does not currently have associations, to create the new associations, you must use the full command syntax in the text file. For the full command syntax for each component, see the associated man page.

When you edit a component that has associations with components that are children of the component you are editing, the text file contains a line for the configuration of the child components that begins with the command **modify**, for example: pools modify { [existing pool members configurations] }. In this case, if you want to add or delete pool members, you must add additional lines to the text file, for example: pools delete { [pool members to delete] }.

If you want the text file that opens to contain all of the editable properties of the component that you want to edit, you must use the **all-properties** option at the end of the **edit** command sequence; otherwise, only the non-default properties display in the text file.

Examples

edit / gtm pool a*

From the **root** module, opens a file in an editor in which you can modify the configuration of all Global Traffic Manager pools with names that start with the letter **a** using the template that displays in the editor.

edit datacenter new_dc

From the **gtm** module, opens a file in an editor in which you can create the Data Center named **new_dc** using the template that displays in the editor.

edit datacenter a*

From the **gtm** module, opens a file in an editor in which you can edit all existing datacenters with names that begin with the letter **a**.

edit datacenter new_datacenter existing_datacenter

From the **gtm** module, opens a file in an editor in which you can create a new datacenter and edit an existing datacenter. Note that when the file opens, a template displays that you can use to create a new datacenter followed by the configuration of the existing datacenter.

edit rule rule_1

From the **gtm** module, opens a file in an editor in which you can create an iRule named **rule_1** using the template that displays in the editor.

When the editor opens, and you are creating or editing an iRule, you must enclose the iRule syntax in brackets, for example, **[...iRule...]**. Note that the template includes the brackets.

Options

- **all**
  Specifies that you want to modify all of the existing components of the specified type.
- **component**
  Specifies the type of component that you want to create or modify.
- **module**
  Specifies the module within which the component resides.
- **name**
  Specifies a unique name of each component that you want to create or modify.

See Also

tmsh

exit

Exits a **tmsh** module or component.

Syntax

Use the command **exit** within a tmsh module or component to leave that module or component and return to the higher level of the shell structure.

```
exit
```

Note that to exit **tmsh** and return to the BIG-IP® system prompt, use the command **quit**.

See Also

tmsh

generate

Generate signed scripts using different algorithms for components (for example, iRules).

Description

Use the **generate** command to generate signed scripts for components. Currently two algorithms are supported: checksum and signature.

```
generate <script_name> checksum
generate <script_name> signature signing-key <key_name>
```

See Also

rule, *template*

help

Displays context-sensitive help text.

Syntax

Use the command **help** within a **tmsh** module to display information about the components that reside within that module, or at the component level to display help about the component. To display help for a component that resides in one module from within another module, use the full path to the component.

Type the question mark (?) character anywhere in **tmsh** to display a list of modules, components, and commands that are available within the module in which you are currently working.

```
?
help
help [module...module]
help [component]
help / [module...module] [component]
help search [text]
```

Description

You can display **tmsh** man pages using the command **help**.

Examples

?

From within the **gtm** module, displays a list of modules, components, and commands that are available.

help pool

From within the **gtm** module, displays help about Global Traffic Manager pools.

help / ltm pool

From within the **gtm** module, displays help about Local Traffic Manager pools.

Options

- **component**
  Specifies the type of the component for which you want to display help.

- **search**
  Use the **search** option to find help topics that contain the specified text. The search is case insensitive. Text that contains a space or special tmsh characters must be quoted. Note that the search will not always find text that spans multiple lines.
- **module**
  Specifies the module within which the component for which you want to display help resides.

See Also

tmsh

install

Install and update components.

Description

Use the command **install** to install or update the following components. For the description and syntax see the help page for each component.

```
sys license
sys software block-device-hotfix
sys software block-device-image
sys software hotfix
sys software image
```

See Also

license, sys software block-device-hotfix, *block-device-image*, *hotfix*, *image*, *tmsh*

list

Displays components that you have permission to view.

Syntax

Use the **list** command within a **tmsh** module to display the properties of the components in that module. To display the properties of the components in one module from within another module, use the full path to the component.

```
list [component]
list [component] [name]
list [component] [name] [property]
list / [module...module] [component] [name] [property]
    all-properties
    current-module
    non-default-properties
    one-line
    partition
    recursive
```

Description

When the default Read partition is **All**, use the **list** command to display all of the components that you have permission to view within a **tmsh** module. When you specify a Read partition, the **list** command displays:

- Only the components that you have permission to view in the current partition
- All of the components that are not in partitions
- All of the components in partition **Common**

Examples

list / ltm

From within the **gtm** module, displays the properties of all of the components in the **ltm** module, including the components in the **ltm monitor**, **ltm persistence**, and **ltm profile** modules.

list / ltm current-module

From within the **gtm** module, displays the properties of all of the components in the **ltm** module, not including the components in the **ltm monitor**, **ltm persistence**, and **ltm profile** modules.

list pool

From within the **gtm** module, displays the properties of all of the Global Traffic Manager pools.

list pool all-properties

From within the **gtm** module, displays all of the properties of all of the Global Traffic Manager pools.

list pool monitor

From within the **gtm** module, displays the monitor associated with each Global Traffic Manager pool.

list / ltm pool

From within the **gtm** module, displays the properties of all of the Local Traffic Manager pools.

Options

- **all-properties**
  Displays the values of all of the properties of the specified component.
- **component**
  Specifies the component that you want to display.
- **current-module**
  Specifies to display only the components that reside in the specified module, not the components that reside in the sub-modules of that module.
  For example, from within the **ltm** module to display only the components in the **gtm** module, and not the components in the **gtm monitor** and **gtm settings** sub-modules, use the following command sequence: **list / gtm current-module**.
- **module**
  Specifies the module within which the component that you want to display resides.

◆ Note

*When you use the command **list** at the module level, by default, the system does not display all of the components that reside in the specified module. To display the properties of some components you must explicitly specify the component. For example, from the **ltm** module, to display the virtual addresses for the Local Traffic Manager, use this command sequence: **list virtual-address***
For more information about displaying the properties of a component, see the man page for the component.

- **name**
  Specifies the unique name of the component.
- **non-default-properties**
  Displays the values of all of the properties for which a user changed the value from the default value for the specified component.

- **one-line**
  Displays the configuration for each object on one line. Configuration that consists of scripts will not be formatted on to a single line. This include ltm and gtm iRules and tmsh scripts.
- **partition**
  Displays the administrative partition within which the specified component exists.
- **property**
  Specifies the property of the component that you want to display.
- **recursive**
  Specifies to display the components not only from the current folder but also from all sub-folders recursively.

See Also

tmsh

load

Replaces the running configuration of the BIG-IP® system with the configuration in the specified files. You can also use this command to import an ASM policy from a file / standard input.

See Also

save, *tmsh*, *policy*, ltm dns dns-express db, *config*, *geoip*, *ucs*

modify

Modifies a **tmsh** component.

Syntax

Use the command **modify** within a **tmsh** module to modify a component that resides in that module. To modify a component in one module from within another module, use the full path to the component.

```
modify [component] [name] [property [value] ]...
modify / [module...module] [component] [name] [property [value] ]...
```

Description

You must provide the name of the component that you want to modify.

You can apply one or more property settings to multiple components using a single command sequence. For example, to associate the Local Traffic Manager pool named **pool-1** with the virtual servers named **virtual-1** and **virtual-2**, use this command sequence: **modify ltm virtual virtual-1 virtual-2 pool pool-1**

Examples

modify pool pool1 disabled

From within the **gtm** module, disables the Global Traffic Manager pool named **pool1**.

modify / ltm pool my_pool disabled

From within the **gtm** module, disables the Local Traffic Manager pool named **my_pool**.

Options

- **component**
  Specifies the type of the component that you want to modify.
- **module**
  Specifies the module within which the component that you want to modify resides.
- **name**
  Specifies the unique name of the component that you want to modify.
- **property [value]...**
  Specifies the properties of the component that you want to modify and their new values.

See Also

tmsh

mv

Renames or moves a TMOS™ configuration object.

Syntax

Use the **mv** command within a **tmsh** module to move or rename the component that resides in that module. To move a component that resides in another module, use the full path to the component.

```
mv [component] [source] [destination]
mv / [module...module] [component] [source] [destination]
```

Description

You must provide a unique name for the source and destination of the move operation.

WARNING Currently MV is an experimental feature. By using this feature, you may be subject to loss of statistics and disruption in GTM service. If you plan to move or rename a Virtual Server, please contact your GTM administrator before doing so. You may enable this feature by setting the appropriate db variable. This can be done by issuing the command:

modify /sys db mcpd.mvenabled value true

This will turn on the feature and allow moving and rename of select objects through TMSH only. Once you have finished using the feature, we recommend disabling it once again. You may do this by issuing the following command:

modify /sys db mcpd.mvenabled value false

Please use responsibly.

Examples

mv cm device bigip seattle32

Renames the device named bigip to seattle32.

mv ltm pool mypool myotherpool

Renames the LTM Pool named mypool to myotherpool.

mv ltm pool /Common/by/mypool /Common/myotherpool /Common/sub/mythirdpool to-folder /Partition2/sub1

Moves the 3 pools in 3 different locations named mypool, myotherpool and mythirdpool into a single folder in another partition.

Options

- **to-folder**
  Specifies the folder to move the item or items into.
- **component**
  Specifies the type of the component that you want to move.
- **destination**
  Specifies a unique name for the component.
- **module**
  Specifies the module within which the component that you want to move resides.
- **source**
  Specifies the component to be moved.

See Also

tmsh

publish

Finalizes changes in the policy by creating a read-only copy of it.

Description

Use the command **publish** to make **wam** policies available for usage in **wam** applications. You can also use this command to apply **asm** policies. For the description and syntax see the help page for **wam policy** or **asm policy**.

See Also

policy, *policy*, *tmsh*

pwd

Display the current working folder.

Syntax

Use the command **pwd** to display the current working folder.

```
pwd
```

Description

Display the current working folder

Examples

pwd

See Also

cd, *help*, *folder*, *tmsh*

quit

Exits **tmsh**.

Syntax

Use the following command at the **tmsh** prompt to close **tmsh** and return to the BIG-IP® system prompt.

```
quit
```

Note that to exit a **tmsh** module or component, you use the command **exit**.

See Also

tmsh

reboot

Reboots the system or boots the system into a different volume.

Syntax

```
reboot
  slot [ [slot number] | all ]
  volume [name]
```

Description

You can use the command **reboot** to reboot the system or cluster. If you do not specify an option, the local system reboots.

You can use the **volume** option to reboot a system into a specific volume. For a cluster, you can use the **volume** option to reboot all slots into the specified volume.

Additionally, for a cluster, you can use the **slot** option to reboot either a specific slot or all slots. Note that the **slot** option does not modify the active volume.

Examples

reboot

Immediately reboots the running image.

reboot volume HD1.2

If the volume HD1.2 has a complete image on it, the system (or cluster) reboots into that image immediately. However, if a software installation is in progress on the volume the system reboots as soon as the installation is complete.

Options

- **slot [[slot number] | all]**
  Reboots either a specific slot or all slots in a cluster, without changing the active volume of the slot(s).
  This option is only available in a clustered environment.

◆ Note

*The **slot** and **volume** options are mutually exclusive.*

- **volume**
  Specifies the volume that you want to boot. The volume you specify becomes the default boot volume. You cannot specify the active volume. In a clustered environment all slots reboot into the same volume.

◆ Note

*The **slot** and **volume** options are mutually exclusive.*

See Also

install, *hotfix*, *image*, *status*, *volume*, *tmsh*

reset-stats

Resets statistics for the specified components.

Syntax

Use the command **reset-stats** within a **tmsh** module to reset the statistics for the specified component to zero. To reset the statistics for the specified component in one module from within another module, use the full path to the component.

```
reset-stats [component]
reset-stats [component] [name]
reset-stats / [module...module] [component]
reset-stats / [module...module] [component] [name]
```

Description

You can reset statistics for a group of components, or you can reset statistics for a specific component.

After you reset statistics, when you run the command **show**, you may see a value of **nan**. This stands for **not a number**, which indicates that no data is currently available. Wait a few moments and run the command **show** again, and in most cases the **nan** value will be replaced by an integer value.

It is important to note the following when you reset statistics:

- For a data center, the system also resets the statistics for the servers in that data center.
- For a Global Traffic Manager server, the system also resets the statistics for the virtual servers on that server.
- For a Global Traffic Manager pool, the system also resets the statistics for the pool members.
- For a Local Traffic Manager pool, the system also resets the statistics for the pool members.
- For a VLAN, you must reset the statistics for the trunks and interfaces associated with the VLAN.
- You cannot reset statistics for system-supplied profiles.

Examples

reset-stats pool

From within the **gtm** module, resets the statistics for all of the Global Traffic Manager pools.

reset-stats pool pool1

From within the **ltm** module, resets the statistics for the Local Traffic Manager pool named **pool1**.

reset-stats / ltm pool my_pool

From within the **gtm** module, resets the statistics for the Local Traffic Manager pool named **my_pool**.

reset-stats all-stats

From within the **sys performance** module, resets all performance statistics for the system.

Options

- **component**
  Specifies the type of the component for which you want to reset statistics.
- **module**
  Specifies the module within which the component for which you want to reset statistics resides.
- **name**
  Specifies the unique name of the component for which you want to reset statistics.

See Also

tmsh

restart

Restarts a service on the BIG-IP® system.

Syntax

Use the command **restart** within **tmsh** to restart a specified service.

```
restart
    /sys service [service name]
```

Description

You can use the command **restart** to restart a specified service.

Examples

restart /sys service mcpd

Restarts the **mcpd** daemon.

restart /sys service snmpd

Restarts the **snmpd** daemon.

Options

Tip: Use the tab completion feature to see a list of available services.

See Also

start, *stop*, *service*, *tmsh*

run

Runs the specified program.

Syntax

Use the **run** command within **tmsh** to run a specified utility.

```
run
    /cli script [arguments]
    /gtm big3d_install [arguments]
    /gtm bigip_add [arguments]
    /gtm gtm_add [arguments]
    /sys config-sync
    /sys config-sync pull
    /util bash [arguments]
    /util dig [arguments]
    /util dnat [arguments]
    /util get-dossier [arguments]
    /util get_ccn_dossier
    /util lsndb [arguments]
    /util sipdb [arguments]
    /util netstat [arguments]
    /util ping [arguments]
    /util ping6 [arguments]
    /util qkview [arguments]
    /util racoonctl [arguments]
    /util sys-icheck [arguments]
    /util tcpdump [arguments]
    /util tracepath [arguments]
    /util tracepath6 [arguments]
    /util traceroute [arguments]
    /util traceroute6 [arguments]
    /wom diagnose-conn
    /wom verify-config
```

Description

You can use the **run** command to run the specified program or utility.

You can read about the arguments that are available for the utilities in the **gtm** module using the following command sequence:

help /gtm [big3d_install | bigip_add | gtm_add]

You can read about the arguments that are available for the utilities in the **util** module using the following command sequence:

help /util [utility name]

◆ Note

*Some **tmsh** features, such as tab completion, context-sensitive help, paging, and grep, are not available for utilities.*

When you are building a batch mode transaction in **tmsh**, if you type the **run** command, the system runs the specified program immediately. It does not add the **run** command to the transaction that you are building.

Examples

help /util ping

Displays the help page for the **ping** utility.

Options

- **big3d_install**
  Specifies to install the **big3d** daemon.
- **bigip_add**
  Specifies the BIG-IP systems that you want to add to the Global Traffic Manager configuration.
- **bash**
  Accesses the system shell.
- **config-sync**
  Synchronizes the configuration of the peer unit to the configuration of the local unit in a redundant pair.
- **config-sync pull**
  Synchronizes the configuration of the local unit to the configuration of the peer unit in a redundant pair.
- **diagnose-conn**
  Runs the specified **diagnose-conn** script, which detects the sources of network connection and performance problems in a WAN optimization configuration.
- **dig**
  Runs the specified **dig** command. The **dig** utility queries DNS name servers.
- **dnat**
  Runs the specified **dnat** command for the purpose of doing forward/reverse mapping of addresses for DNAT.
- **sipdb**
  Displays **SIP** persistence entries. The **sipdb** utility displays specific persistence entries and delete a particular persistence record.
- **get-dossier**
  Runs the **get_dossier** utility for the purpose of displaying system license dossier information.
- **get-ccn-dossier**
  Runs the **get_ccn_dossier** utility for the purpose of displaying system information for dossier creation.

- **gtm_add**
  Specifies the Global Traffic Manager systems that you want to add to the Global Traffic Manager configuration.
- **netstat**
  Displays network connections, routing tables, interface statistics, masquerade connections, and multicast memberships.
- **ping**
  Runs the specified **ping** command. The **ping** utility sends ICMP echo requests to network hosts.
- **ping6**
  Runs the specified **ping6** command. The **ping6** utility sends ICMPv6 echo requests to network hosts.
- **qkview**
  Runs the specified **qkview** command. The **qkview** utility gathers diagnostic information from a BIG-IP system.
- **racoonctl**
  Runs the specified **racoonctl** command. The **racoonctl** utility is used to control operation of the **racoon** daemon.
- **ssh-keyswap**
  Runs the **keyswap.sh** script for managing SSH keys on the BIG-IP.
- **sys-icheck**
  Runs the specified **sys-icheck** command. The **sys-icheck** utility verfiies all RPM packages and files.
- **tcpdump**
  Runs the specified **tcpdump** command. The **tcpdump** utility prints headers and content of network traffic.
- **tracepath**
  Displays the route packets take to a network host.
- **tracepath6**
  Displays the route packets take to an IPv6 network host.
- **traceroute**
  Displays the route packets take to a network host.
- **traceroute6**
  Displays the route packets take to an IPv6 network host.
- **verify-config**
  Runs the specified **verify-config** script, which detects errors in the configuration of the WAN Optimization Manager.

See Also

script, gtm big3d_install, gtm bigip_add, gtm gtm_add, sys config-sync, *tmsh*, util bash, util dig, *dnat*, util netstat, util ping, util ping6, util qkview, util racoonctl, util tcpdump

save

Writes the running configuration of the BIG-IP® system to the specified file.

Description

You can use the **save** command to write changes that you make to the running configuration of the BIG-IP system to the specified file. You can also use this command to save an analytics report to a file on the BIG-IP® system or to export an ASM policy to a file / standard output.

See Also

report, *policy*, *load*, *config*, *ucs*, *tmsh*

send-mail

Send an e-mail to a list of recipients containing configuration or statistical information about the BIG-IP® system.

Descriprion

You can use the **send-mail** command to send an analytics report from the BIG-IP system to a list of e-mail recipients.

See Also

report, *tmsh*

show

Displays statistics for and the status of specified components.

Syntax

Use the **show** command within a **tmsh** module to display statistics for and the status of components in that module. To display statistics for and the status of components in another module, use the full path to the component.

```
show
show [component]
show [component] [name]
show / [module] [component] [name]
    all-stats
    current-module
    (default | exa | gig | kil | meg | peta | raw | tera | yotta | zetta)
    (detail | global | historical)
    field-fmt
    running-config
    recursive
```

Description

You can use the **show** command to specify the unit value in which the system displays statistics and the type of statistics that you want the system to display.

After you reset statistics, when you run the command **show**, you may see a value of **nan**. This stands for **not a number**, which indicates that no data is currently available. Wait a few moments and run the **show** command again, and in most cases the **nan** value is replaced by an integer value. For more information, see **help reset-stats**.

Examples

show / ltm current-module

From within the **gtm** module, displays statistics and status for all the components within the **ltm** module, but not the components in the **ltm monitor**, **ltm persistence**, and **ltm profile** modules.

show pool

From within the **gtm** module, displays statistics and status for all Global Traffic Manager pools.

show pool pool1

From within the **gtm** module, displays statistics and status for the Global Traffic Manager pool named **pool1**.

show / ltm pool

From within the **gtm** module, displays statistics and status for all Local Traffic Manager pools.

show / ltm profile tcp global

From within the **gtm** module, displays global statistics and status for all Local Traffic Manager TCP profiles in the system default unit.

Options

- **all-stats**
  Displays all of the available system performance statistics.
- **component**
  Specifies the type of the component for which you want to show statistics and status.
- **current-module**
  Specifies to display only the components that reside in the specified module, not the components that reside in the sub-modules of that module.
  For example, from within the **ltm** module to display only the components in the **gtm** module, and not the components in the **gtm monitor** and **gtm settings** sub-modules, use this command sequence: **show / gtm current-module**.
- **default**
  Displays data in the simplest units. For example, if the value of the data is 1,200,001, the system displays 1.20M; however, if the value of the data is 1,200, the system displays 1.2K.
- **detail**
  Displays detailed data for the specified component and associated components. Note that this option is available for only a partial set of **tmsh** components.
  You can use the tab completion and context-sensitive help features to determine if this option is available. For more information about these features, see **help**.
- **field-fmt**
  Displays data as a list of options and their values. The option names can be used to retrieve statistics and status values in a shell script, see **cli script**.
- **gig**
  Displays data in parts per billion.
- **global**
  Displays global statistics for the specified component that includes statistics for all components of the specified type. Note that this option is available for only a partial set of **tmsh** components. You can use the tab completion and context-sensitive help features to determine if this option is available.

- **historical**
  Displays historical statistics for the specified component. Note that this option is available only for a partial set of **tmsh** components. You can use the tab completion and context-sensitive help features to determine if this option is available.
- **kil**
  Displays data in parts per thousand.
- **lines**
  Specifies how many lines of the log that you want the system to display.
- **meg**
  Displays data in parts per million.
- **module**
  Specifies the module within which the component for which you want to show statistics and status resides.

Note

*When you use the command **show** at the module level, by default, the system does not display all of the components that reside in the module. To display some components you must explicitly specify the component. For example, from the **ltm** module, to display the statistics for and status of the virtual addresses of the Local Traffic Manager, use the following command sequence:*
show virtual-address
For more information about displaying statistics for and status of a component, see the man page for the component.

- **name**
  Specifies the unique name of the component for which you want to show statistics and status.
- **range**
  Specifies a date range for the logs that you want the system to display, for example:
  - **2d-4d**
    Specifies 2 - 4 days ago.
  - **3d**
    Specifies 3 days ago to now.
  - **epoch--7/25:12:00:00**
    Specifies everything older than July 25th at noon.
  - **2008-07-25--2008-07-28:13:30**
    Specifies between July 25th and 28th at 1:30 p.m.
- **raw**
  Displays raw data.
- **recursive**
  Specifies to display the components not only from the current folder, but also from all sub-folders recursively.

- **running-config**
  Displays the running configuration of the components that you have permission to view within a **tmsh** module, if the default Read partition is **All**. If you specify a Read partition, this option displays only the components that you have permission to view in the current partition, all of the components that are not in partitions, and all of the components in partition Common. Note that this option is valid only for **tmsh** components you can configure.
  The **running-config** option must be specified immediately after the **show** command, for example:

show running-config ltm pool

See Also

script, *tmsh*

shutdown

Shuts down the system.

Syntax

```
shutdown
  slot [ [slot number] | all ]
```

Description

You can use the command **shutdown** to power down the system or cluster. If you do not specify an option, the local system shuts down.

For a cluster, you can use the **slot** option to shut down either a specific slot or all slots.

Examples

shutdown

Immediately shuts down the running system.

Options

- **slot [[slot number] | all]**
  Shuts down either a specific slot or all slots in the cluster. This option is only available in a clustered environment.

See Also

reboot, *install*

start

Starts a service on the BIG-IP® system.

Syntax

Use the **start** command within **tmsh** to restart a specified service.

```
start
    /sys service [service name]
```

Description

You can use the **start** command to start a specified service.

Examples

start /sys service mcpd

Starts the **mcpd** daemon.

start /sys service snmpd

Starts the **snmpd** daemon.

Options

Tip: Use the tab completion feature to see a list of available services.

See Also

restart, *stop*, *service*, *tmsh*

stop

Stops a service that is running on the BIG-IP® system.

Syntax

Use the command **stop** within **tmsh** to stop a running service.

```
stop
    /sys service [service name]
```

Description

You can use the command **stop** to stop a running service.

Examples

stop /sys service mcpd

Stops the **mcpd** daemon.

stop /sys service snmpd

Stops the **snmpd** daemon.

Options

Tip: Use the tab completion feature to see a list of available services.

See Also

restart, *start*, *service*, *tmsh*

submit

Runs the transaction that you are creating.

Syntax

Use the **submit** command to run a transaction that you are creating.

```
submit transaction
```

Description

You can use the **submit** command to run a transaction, which is a series of commands that you enter in transaction mode.

For more information about creating transactions, see **cli transaction**.

See Also

transaction, *tmsh*

time

Date and Time formats.

Syntax

Date/Time Syntax

```
now[ [ + | - ] <integer> [ d | h | w | m ] ]
yyyy-mm-dd[ : | T ]hh:mm[:ss]
mm-dd[-yyyy][ : | T ]hh:mm[:ss]
mm/dd[/yyyy][ : | T ]hh:mm[:ss]
```

Date Range Syntax

```
now[ [ + | - ] <integer> [ d | h | w | m ] ]--now[ [ + | - ] <integer> [ d | h | w | m
] ]
yyyy-mm-dd[ : | T ]hh:mm[:ss]--yyyy-mm-dd[ : | T ]hh:mm[:ss]
mm-dd[-yyyy][ : | T ]hh:mm[:ss]--indefinite
epoch--mm/dd[/yyyy][ : | T ]hh:mm[:ss]
now[ [ + | - ] <integer> [ d | h | w | m ] ]
```

Description

The **date** or **time** format is found in **tmsh** as an attribute or parameter for many configuration items. Below are the various formats supported for both **Date / Time** and **Date Range**. Please see the examples for further assistance in using the required formats.

Date:Time Formats

- **nowX**
  This date format starts with **now** (the current time) and is *optionally* followed by **+** or **-** some time span. The format will look like the following: **now[[+ | -] integer [d | h | w | m]]**, where the user picks either before (**-**) or after (**+**) the current time and then specifies **integer** number of **minutes** (m), **hours** (h), **days** (d) or **weeks** (w). This format is **case-insensitive**.
  - **Examples:**

Input Date	Description
now-3d	3 days ago.
now+3h	3 hours from now.
now-3m	3 minutes ago.
now+3w	3 weeks from now.

- **yyyy-mm-dd:hh:mm:ss**
  This format requires a **year**, **month**, **day** separated by **-** characters. A **time** is also required, which is specified as **hour**: **minute**: **second**, where the **seconds** are optional. The **date** and **time** must be separated by a **:** colon. **Note:** This is the default time format for output from tmsh.
  - **Examples:**

```
Input Date              Description
2013-05-29:13:30        May 29th, 2013 at 1:30pm.
2000-01-04:12:22:30     January 4th, 2000 at 12:22pm and 30 seconds.
```

- **mm-dd-yyyy:hh:mm:ss**
  This format requires at least a **month** (m) and **day** (d) specified and optionally a **year** (y). If no year is specified, **tmsh** will auto-fill the year with the current year. A time is also required in the format of **hour**: **minute**: **second**, where the **seconds** are optional.
  - **Examples:**

```
Input Date              Description
3-12-2015:12:01:00      March 12th, 2015 at 12:01 pm.
4-15:22:10:30           April 15th of this year at 10:10 pm and 30 seconds.
```

- **mm/dd/yyyy:hh:mm:ss**
  This format requires at least a **month** (m) and **day** (d) specified and optionally a **year** (y). If no year is specified, **tmsh** will auto-fill the year with the current year. A time is also required in the format of **hour**: **minute**: **second**, where the **seconds** are optional.
  - **Examples:**

```
Input Date              Description
3/12/2015:12:01:00      March 12th, 2015 at 12:01 pm.
4/15:22:10:30           April 15th of this year at 10:10 pm and 30 seconds.
```

- **T Delimiter**
  Any of the above time formats may optionally use a capital letter **T** (as in the word Time) to separate the **date** from the **time**, instead of using a **colon** (:).
  - **Examples:**

```
Input Date              Description
9/16/2005T12:01:01      September 16th, 2005 at 12:01pm and 1 second.
2011-11-12T00:03:30     November 12th, 2011 at 12:03am and 30 seconds.
```

- **Special Dates**
  There are two special dates that may be used in **tmsh**. They are **indefinite** and **epoch**. Below is an explanation of those dates.
  - **indefinite**
    The date will be marked as being infinitely in the future (end of time).
  - **epoch**
    The date will be marked as being infinitely in the past (beginning of time).

Date Ranges

- **DateX--DateZ**
  A **Date Range** is 2 **dates** in a valid **Date Format** separated by a **--** (double hyphen). The **dates** may be any of the **Date Formats** specified above. See examples below on how to use this notation.
  - **Examples:**

```
Input Date                  Description

now-2d--now-4d              2 to 4 days ago.
now--now-3m                 From 3 minutes ago to now.
epoch--3/12/2011:12:00:00   Everything older than March 12th, 2011 at noon.
2008-03-12--indefinite      Everything after midnight on March 12th, 2008.
```

- **DateX**
  When specifying a date range, the second date may be left out. This will cause the system to assume the second date in the range to be **now**. Using this format for a date range may make it confusing when using the **NowX** date format listed above. The following examples will help clarify how to use this format with any supported **Date Format**.
  - **Examples:**

```
Input Date      Description

now-3d          From 3 days ago to now.
now+3w          From now to 3 weeks from now.
epoch           Everything before the current date and time.
indefinite      Everything after the current date and time.
```

See Also

tmsh, *create*, *modify*

tmsh

Traffic Management Shell - A command line interface for managing the BIG-IP® system.

Description

You can use **tmsh** to configure and manage the BIG-IP system in conjunction with the Configuration utility, which is the browser-based BIG-IP system and network management tool.

Modules

The structure of **tmsh** is hierarchical and modular. The highest level is the **root** module, which contains subordinate modules: **auth**, **cli**, **gtm**, **ltm**, **net**, **sys** and **wom**. Use the command **help** with no arguments to display the module hierarchy relative to the current module.

The **gtm**, **ltm**, **net**, **sys**, and **wom** modules also contain subordinate modules. All modules and subordinate modules contain components. To display the list of modules and components that are available in the current module type **Tab** or **?** at the **tmsh** prompt.

Commands operate on components. To display the list of available commands type **Tab** or **?** at the beginning of the command line. To display a list of components on which a command can operate type the command followed by a space followed by **Tab** or **?**.

The following examples illustrate how to navigate the **tmsh** hierarchy.

To enter a module, type the name of the module at the **tmsh** prompt.

```
(tmos)# ltm
```

The prompt displays the current module location.

```
(tmos.ltm)#
```

You can display the components in a module using the commands **list** (configuration) and **show** (statistics and runtime status). The following command sequence displays the virtual server configuration of the BIG-IP system.

```
(tmos.ltm)# list virtual
```

In the following examples, the commands list and show display information about only **ltm** components.

```
(tmos.ltm)# list
(tmos.ltm)# show
```

You can access any component in any module from any other module by specifying a complete path to the component. For example, from the **ltm** module, the following command displays all of the properties of the VLANs on the system. The forward slash **/** specifies that what follows is relative to the root module.

```
(tmos.ltm)# list /net vlan all-properties
```

The forward slash is optional if the **root** module is the current module. For example, the following command sequences display profiles.

```
(tmos)# list ltm profile
(tmos)# list /ltm profile
(tmos)# list / ltm profile
```

Most components also support **component** mode. You can navigate to a single component and run commands to manage that component. For example, from the **ltm** module, to navigate to the **node** component, use the following command.

```
(tmos.ltm)# node
```

To display the properties of all nodes, use the following command.

```
(tmos.ltm.node)# list
```

You can also navigate to a specific object (object mode). For example, from the **node** component, to enter object mode for a specific node, enter the command **modify** followed by the IP address of the node.

```
(tmos.ltm.node)# modify 10.1.1.10
```

In object mode, you can configure property settings directly. For example, to set the connection limit for **10.1.1.10** to **10000**, use the following command.

```
(tmos.ltm.node.10.1.1.10)# connection-limit 10000
```

To exit a module enter the command **exit** at the **tmsh** prompt, as shown below.

```
(tmos.ltm)# exit
(tmos)#
```

Product Provisioning

You must provision a BIG-IP system module before you can use **tmsh** to configure that product, for example, the Global Traffic Manager. The command sequence **list sys provision** displays the BIG-IP system modules that can be provisioned. For more information about provisioning, see the **TMOS® Management Guide for BIG-IP Systems** and **help sys provision**.

Loading/Saving The System Configuration

The system applies all configuration changes that you make from within **tmsh** to the running configuration of the system.

You can save a portion of the running configuration known as the base configuration. You can also load the base configuration from the stored configuration files.

- To save the base configuration to the stored configuration files, use the command sequence: **save sys base-config**.

- To replace the running base configuration with the configuration in the stored configuration files, use the command sequence: **load /sys base-config**.

Additionally, you can save the entire running configuration or load all of the stored configuration files.

- To save the entire running configuration to the stored configuration files, use the command sequence: **save /sys config**.

- To replace the entire running configuration with the configuration in the stored configuration files using the command sequence: **load /sys config**.

Help

tmsh tmsh includes man pages for each of the commands and components that are available within **tmsh**. You access the man pages using the following command syntax: **help [[command] | [full path to component]]**.

For example, to access the man page for the **vlan** component from the **root** module, use this command sequence: **help / net vlan**.

You can also search the man pages for information on a specific topic. To do this you use the command syntax: **help search [topic]**. You can perform a help search from within any module in the **tmsh** hierarchy. For example, to find the man pages that contain a reference to VLANs, use this command sequence: **help search vlan**

To display a list of topics that are available in a module use this command sequence: **help [full path to module]**.

For example, to display the topics that are available in the current module use this command: **help**. To display the topics that are available in the **net** module use this command sequence: **help / net**.

Context-Sensitive Help

tmsh includes a context-sensitive help feature that provides help as you type commands. At any time, you can type a question mark (**?**) on the command line, and **tmsh** returns information to assist you in completing the command. Based on when you type the question mark, you get the following results.

- When you type a question mark immediately following any portion of a command, **tmsh** returns possible completions for the command, but does not complete the command as the command completion feature does.

- When you type a space before the question mark, **tmsh** returns descriptive text that explains the commands, components, or properties that you can configure.

- When you type a question mark in the middle of a command, **tmsh** returns help on the command to the left of the cursor.

◆ Note

To use a question mark in a Glob or regular expression, you must escape the question mark using quotation marks, apostrophes, or a backslash.

Additionally, you can request context-sensitive help for the last command in a series of commands. For more information, see ENTERING MULTIPLE COMMANDS, following.

Command Completion

At any point while typing or editing a command in **tmsh**, you can press the **Tab** key. **tmsh** either completes the current or next word, or displays possible completions for the current or next word. If **tmsh** displays nothing after you press the **Tab** key, no options exist to complete the word. If you move the cursor anywhere on the command line and press the **Tab** key, **tmsh** completes what is to the left of the cursor.

Command completion also reduces the amount of typing that is required to run commands. When you press the Tab key, the system automatically completes the current command-line element to as many unique characters as possible. If there is more than one possible completion the list of possible completions displays. Command completion also completes configuration object identifiers.

Entering Multiple Commands

You can enter multiple commands on the command line by separating the commands with semi-colons (;). For example, to display the properties of the self IP addresses and VLANs of the system, use this command sequence:

```
list / net self ; list / net vlan
```

When you enter multiple commands in this way, all of the commands are added to the command history in a single line item, regardless of whether any of the commands were successful. However, if one of the commands that you enter fails to parse, tmsh does not run the remaining commands you entered. tmsh audits commands as the commands run; therefore, if a command fails to parse, tmsh does not audit the remaining commands. For more information about the command history, see COMMAND HISTORY, following.

You can also specify multiple commands in a command alias by separating the commands with semi-colons. For example, to create an alias that displays the properties of the VLANs and VLAN groups on the system, use this command sequence:

```
create / cli alias vlans command "list / net vlan ; list / net vlan-group"
```

You can request context-sensitive help and utilize the command completion feature on the last command in a series of commands. For example, the following command sequence displays help for the **vlan-group** component.

```
list / net vlan ; list / net vlan-group ?
```

Command History

tmsh saves in the command history file each command that you enter. The command history persists when you log off of the system. The next time you log on to the system, you can search for, display, and then edit, the **tmsh** commands that you entered in previous sessions. The command history persists even through a restart of the BIG-IP system. For more information about the command history feature, see **help history**.

The following examples show how to use the command history feature.

To display the commands in the history list, enter either the command sequence **show history** or an exclamation point (!). **tmsh** displays a list of commands each preceded by a numeric ID.

To run a command from the history list, enter an exclamation point followed by the numeric ID of the command.

To run the previous command, enter **!!**.

Filtering Output

You can filter the output generated by the commands **list** (configuration settings) and **show** (statistics and runtime status) using the UNIX grep utility. You must type the character | before the grep specification. You can use multiple filters chained together.

The following examples show how to use the grep utility in **tmsh**.

```
list ltm node | grep "^10.2"
list ltm virtual | grep -i seattle
list ltm virtual | grep -i abc | grep -i ab | grep -i a
```

Keyboard Bindings

tmsh supports vi, emacs and default keyboard bindings. You can set the binding using the **keymap** preference. For more information, see **help cli preference**.

Note that all mappings provide command-line editing and the capability to search the command history.

Wildcard Object Identifiers

You can specify configuration object identifiers using glob and regular expression syntax.

For glob and regular expression syntax rules, see **help glob** and **help regex**. Note that you can escape the glob and regular expression special characters using a back slash.

The following examples show how to use glob and regular expressions in **tmsh**.

Uses a glob expression to display the configuration of all nodes that begin with **10.1.**.

```
list ltm node 10.1.*
```

Uses a regular expression to display the configuration of all nodes that begin with **10.** and contain **.44.**. Note that a regular expression must begin with an @ symbol. This identifies to **tmsh** that the identifier should be treated as a regular expression and not a glob or standard object identifier. The leading @ is not part of the regular expression.

```
list ltm node @^10..*.44.
```

Preferences

You can customize the behavior of **tmsh**. For more information, see **help cli preference**.

Files

tmsh manages several files in a user's home directory.

- $HOME/.tmsh-history-<user> contains command history.

Statistics

You can use **tmsh** to display statistics, including historical performance statistics. You can select the format in which the statistics display, as well as reset the statistics for some of the **tmsh** components. To determine if statistics are available for a component, see the man page for the specific component.

The following examples show how to display and reset statistics for the **net interface** component from the **root** module.

```
show net interface
reset-stats net interface
```

The following examples show how to display and reset statistics for the **net interface** component from the **net** module.

```
show interface
reset-stats interface
```

Automating Tmsh

You can use **tmsh** to build TCL scripts to automate management of the BIG-IP. See the **cli script** help page.

Command Line Options

The following options can be specified when **tmsh** is started from the system shell.

- -a
  tmsh does not write commands to the command history file.
  Note that if auditing is **enabled**, **tmsh** continues to write commands to the audit log. This option is useful when writing scripts from the system shell, because it stops the scripts from filling up the command history file. This option applies to the non-interactive mode only.
- -c
  Run the specified command. A command that contains multiple arguments must be in quotes. No other options may be specified after **-c**
- -d [ip address | host name]
  Connects to the specified blade in a clustered system.
- -e
  Disables video highlighting in **tmsh**.
- -h
  Displays options you can use when accessing **tmsh** from the system shell.
- -m
  Generates a **tmsh** debug log named **tmsh.out** in the current directory.
  Note that when you run a **tmsh** script, the shell generates a debug log file for the script named **tmsh.out.[script name]**.
  Using this option causes **tmsh** to run significantly slower.
- -q
  Prevents **tmsh** from responding to user actions with questions. This option is useful when writing non-interactive shell scripts from the system shell.
- -r <version>
  This option allows the user to run TMSH the specified **version**. This is used to provide backwards compatibility for older TMSH syntax only. The **version** must be specified in the format **maj.min.pt**, for example **11.5.0**

See Also

Detailed information on the following topics is available through the *help* command: *preference*, *script*, glob, *help*, regex, and *provision*.

4

analytics

- Introducing the analytics module
- Alphabetical list of components

Introducing the analytics module

You can use the tmsh components that reside within the analytics module to generate analytics reports. For more information about the tmsh hierarchical structure, see Chapter 2, *Understanding and Using the Traffic Management Shell*.

Alphabetical list of components

The remainder of this chapter lists the tmsh components that are available in the analytics module.

report

Displays an HTTP analytics report. This command is identical to **analytics http report**.

Syntax

Show, save or send an **analytics report** using the syntax shown in the following sections.

Display

```
show report view-by [ application | virtual | pool-member | url |
                      client-ip | country | response-code |
                      method | user-agent | subnet ]
  drilldown {
    {
        entity [ application | virtual | pool-member | url |
                 client-ip | country | response-code | method |
                 user-agent | subnet ]
        values
        {
          [value ...]
        }
    } ...
  }
  field-fmt
  include-total
  include-others
  limit [number of rows]
  measures {
    [measure name ...]
  }
  order-by {
    {
      measure [ measure name ]
      sort-type [ asc / desc ]
    } ...
  }
  range [date range]
```

Save

```
save report view-by [ application | virtual | pool-member | url |
                      client-ip | country | response-code |
                      method | user-agent | subnet ]
   drilldown {
    {
        entity [ application | virtual | pool-member | url |
                 client-ip | country | response-code | method |
                 user-agent | subnet ]
        values
        {
          [value ...]
        }
    } ...
```

```
  }
  file [ file name ]
  format [ csv-aggregated | csv-time-series | pdf ]
  include-total
  include-others
  limit [number of rows]
  measures {
    [measure name ...]
  }
  order-by {
    {
      measure [ measure name ]
      sort-type [ asc / desc ]
    } ...
  }
  range [date range]
```

Send

```
send-mail report view-by [ application | virtual | pool-member |
                           url | client-ip | country | response-code |
                           method | user-agent | subnet ]
  drilldown {
    {
        entity [ application | virtual | pool-member | url | client-ip |
                 country | response-code | method | user-agent | subnet ]
        values
        {
          [value ...]
        }
    } ...
  }
  email-addresses {
     [email address ...]
  }
  format [ csv-aggregated | csv-time-series | pdf ]
  include-total
  include-others
  limit [number of rows]
  measures {
    [measure name ...]
  }
  order-by {
    {
      measure [ measure name ]
      sort-type [ asc / desc ]
    } ...
  }
  range [date range]
  smtp-config-override [ smtp configuration object name ]
```

Description

Use this command to generate HTTP analytics reports. You can generate an HTTP analytics report for the following entities:

- **application** - Application services.

- **virtual** - Virtual servers.
- **pool-member** - Pool members.
- **url** - A URL accessed by HTTP or HTTPs.
- **client-ip** - A single client identified by an IP address.
- **country** - A country from which HTTP/HTTPs traffic was sent to each of the virtual servers.
- **response-code** - An HTTP response code that was sent back to the client.
- **method** - An HTTP method used by the client (GET, CREATE, POST, DELETE, and so on).
- **user-agent** - A browser identifier sent by the client's browser as part of the request for URL.
- **subnet** - Client IP addresses classified into subnets.

Different measures are collected for each of these entities and can be a part of the report request.

Examples

show analytics report view-by virtual measures {average-tps} limit 20

Gets the average tps of 20 virtual servers (unordered).

show analytics report view-by virtual measures {average-tps} limit 20 order-by { { measure average-tps sort-type desc } }

Gets the average tps of the top 20 virtual servers.

show analytics report view-by virtual measures {average-tps} limit 20 order-by { { measure average-tps sort-type desc } } range now-3d--now

Gets the average tps of the top 20 virtual servers from the last three days.

show analytics report view-by virtual drilldown { { entity application values { app } } { entity pool-member values { p1 p2 } } } range now-4d--now-2d measures {average-tps} limit 10 order-by { { measure average-tps sort-type DESC } }

Gets the average tps of the top 10 virtual servers (ordered by average tps) on **app** iApp (out of several monitored) on pool members **p1** and **p2**

show analytics report view-by response-code drilldown { { entity virtual values { v1 } } } measures { transactions }

Gets a distribution of requests per response code on virtual v1.

show analytics report view-by country drilldown { { entity application values { app } } } measures { average-concurrent-sessions average-sessions } order-by { { measure average-sessions sort-type DESC } } limit 5

Gets the new sessions and average concurrent sessions of the top five countries, ordered by the average concurrent sessions on the application **app**.

show analytics report view-by client-ip drilldown { { entity virtual values { v1 } } } measures { max-page-load-time } limit 1

Gets the client IP address with the worst page load time.

show analytics report view-by application drilldown { { entity pool-member values { p1 p2 } } } measures { transactions } order-by { { measure transactions } } range now-7d--now

Gets the distribution of requests per application on pool members *p1*

save analytics report view-by virtual measures {average-tps} limit 20 order-by { { measure average-tps sort-type desc } } format pdf file report.pdf

Gets the average tps of the top 20 virtual servers and exports to a PDF file on the BIG-IP system.

save analytics report view-by virtual measures {average-tps} limit 20 order-by { { measure average-tps sort-type desc } } format csv-aggregated file report.csv

Gets the average tps of the top 20 virtual servers and exports to a CSV file on the BIG-IP system.

save analytics report view-by virtual measures {average-tps} limit 20 order-by { { measure average-tps sort-type desc } } format csv-time-series file report.csv

Gets the average tps over time of the top 10 virtual servers and exports to a CSV file on the BIG-IP system.

send-mail analytics report view-by virtual measures {average-tps} limit 20 order-by { { measure average-tps sort-type desc } } format pdf email-addresses { some.one@someaddress.com }

Gets the average tps over time of the top 10 virtual servers and sends out an email containing the report as a PDF.

Options

- **device**
  Specifies a BIG-IP device on which to generate a report. (Enterprise Manager only)
- **device-list**
  Specifies a custom list of BIG-IP devices on which to generate a report. (Enterprise Manager only)
- **drilldown**
  Specifies entities that are used as a filter.

- **email-addresses**
  Specifies the list of email addresses to which the report file is sent when using the **send-mail** command.
- **file**
  Specifies the exported file path to be saved when using the **save** command. The file name should be simple (not a full path).
- **format**
  Specifies the exported file format to be saved or sent. This option must be specified when using the **save** or **send-mail** commands.
- **include-others**
  Specifies that the grand total for the measure is displayed for all entities, except for those shown in the result. It can be used along with **include-total**.
- **include-total**
  Specifies that a total summary row should be added to the analytics report. For average measures, the total value is also an average.
- **limit**
  Specifies the maximum number of rows/entities in the output result set/file. The default value is **10**, not including the total row/entity. The maximum value is **1000**.
- **measures**
  Specifies a list of measures that can be used with the chosen entity type. The default value is **transactions**. The options are:
  - **average-concurrent-sessions**
    The average number of concurrent sessions for each entity.
  - **average-new-sessions**
    The average number of new sessions for each entity.
  - **average-page-load-time**
    The average client page load time for each entity.
  - **average-request-throughput**
    The average request throughput for each entity.
  - **average-response-throughput**
    The average response throughput for each entity.
  - **average-server-latency**
    The average server latency for each entity.
  - **average-tps**
    The average number of transactions per second for each entity.
  - **client-side-sampled-transactions**
    The number of transactions sampled for client side page load time.
  - **max-page-load-time**
    The maximum client page load time for each entity.
  - **max-request-throughput**
    The maximum request throughput for each entity.
  - **max-response-throughput**
    The maximum response throughput for each entity.

  - **max-server-latency**
    The maximum server latency for each entity.
  - **max-tps**
    The maximum number of transactions per second for each entity.
  - **transactions**
    The absolute number of transactions for each entity.

- **order-by**
  Specifies the measures and sort type (ascending or descending) that will be used to sort the final report. The default value for measures is previously chosen measures. The default value for sort type is **desc** (descending).
- **range**
  Specifies the time/date range of the analytics information that you want to display. The given results will reflect the time range chosen here. The default value is the last hour (now--now-1h).
- **smtp-config-override**
  Specifies the SMTP configuration to use when sending reports by email. This overrides the default SMTP settings.

See Also

show, *save*, *send-mail*, *tmsh*, *analytics*, *report*

5

analytics application-security

- Introducing the analytics application-security module
- Alphabetical list of components

Introducing the analytics application-security module

You can use the tmsh components that reside within the analytics application-security module to generate analytics reports. For more information about the tmsh hierarchical structure, see Chapter 2, *Understanding and Using the Traffic Management Shell*.

Alphabetical list of components

The remainder of this chapter lists the tmsh components that are available in the analytics application-security module.

report

Displays an application-security analytics report.

Syntax

Show, save or send an **analytics application-security report** using the syntax shown in the following sections.

Display

```
show report view-by [ application | virtual | request-type | severity | rating |
username | attack-type | ip-address-intelligence | policy
                        response-code | ip | violation | country | method | protocol |
session-id | url | virus  ]
  drilldown {
    {
        entity [ application | virtual | request-type | severity | rating | username |
attack-type | ip-address-intelligence | policy
                 response-code | ip | violation | country | method | protocol |
session-id | url | virus ]
        values
        {
          [value ...]
        }
    } ...
  }
  field-fmt
  include-total
  include-others
  limit [number of rows]
  measures {
    [measure name ...]
  }
  order-by {
    {
      measure [ measure name ]
      sort-type [ asc / desc ]
    } ...
  }
  range [date range]
```

Save

```
save report view-by [ application | virtual | request-type | severity | rating |
username | attack-type | ip-address-intelligence | policy
                        response-code | ip | violation | country | method | protocol |
session-id | url | virus  ]
   drilldown {
    {
        entity [ application | virtual | request-type | severity | rating | username |
attack-type | ip-address-intelligence | policy
                 response-code | ip | violation | country | method | protocol |
session-id | url | virus ]
        values
        {
          [value ...]
```

```
      }
    } ...
  }
  file [ file name ]
  format [ csv-aggregated | csv-time-series | pdf ]
  include-total
  include-others
  limit [number of rows]
  measures {
    [measure name ...]
  }
  order-by {
    {
      measure [ measure name ]
      sort-type [ asc / desc ]
    } ...
  }
  range [date range]
```

Send

```
send-mail report view-by [ application | virtual | request-type | severity | rating |
username | attack-type | ip-address-intelligence | policy
                          response-code | ip | violation | country | method | protocol
| session-id | url | virus  ]
  drilldown {
    {
       entity [ application | virtual | request-type | severity | rating | username |
attack-type | ip-address-intelligence | policy
                response-code | ip | violation | country | method | protocol |
session-id | url | virus ]
       values
       {
         [value ...]
       }
    } ...
  }
  email-addresses {
     [email address ...]
  }
  format [ csv-aggregated | csv-time-series | pdf ]
  include-total
  include-others
  limit [number of rows]
  measures {
    [measure name ...]
  }
  order-by {
    {
      measure [ measure name ]
      sort-type [ asc / desc ]
    } ...
  }
  range [date range]
  smtp-config-override [ smtp configuration object name ]
```

Description

Use this command to generate application-security analytics reports. You can generate an application-security analytics report for the following entities:

- **application** - Application services.
- **virtual** - Virtual servers.
- **request-type** - Request types (Legal/Alarmed/Blocked).
- **severity** - Violation severities.
- **rating** - Violation ratings.
- **username** - User names.
- **attack-type** - Attack type of the illegal request.
- **ip-address-intelligence** - IP Address reputation categories.
- **policy** - Security policy.
- **response-code** - Response codes.
- **ip** - Source IP addresses.
- **violation** - Violation types.
- **country** - Countries of the source IP address.
- **method** - HTTP methods.
- **protocol** - Protocols (HTTP/HTTPS).
- **session-id** - IDs of sesssions.
- **url** - Requested URLs.
- **virus** - Viruses that were detected by the system.

Different measures are collected for each of these entities and can be a part of the report request.

Examples

show analytics application-security report view-by violation

show analytics application-security report view-by violation drilldown { { entity severity values { Error } } }

send-mail analytics application-security report view-by ip measures {requests} limit 20 order-by { { measure requests sort-type desc } } format pdf email-addresses { some.one@someaddress.com }

For more syntactical examples see manual for **analytics report**.

Options

- **device**
  Specifies a BIG-IP device on which to generate a report. (Enterprise Manager only)
- **device-list**
  Specifies a custom list of BIG-IP devices on which to generate a report. (Enterprise Manager only)
- **drilldown**
  Specifies specific entities that are used as a filter.
- **email-addresses**
  Specifies the list of email addresses to which the report file is sent when using the **send-mail** command.
- **file**
  Specifies the exported file path to be saved when using the **save** command. The file name should be simple (not a full path).
- **format**
  Specifies the exported file format to be saved or sent. This option must be specified when using the **save** or **send-mail** commands.
- **include-others**
  Specifies that the grand total for the measure is displayed for all entities, except for those shown in the result. It can be used along with **include-total**.
- **include-total**
  Specifies that a total summary row should be added to the analytics report. For average measures, the total value is also an average.
- **limit**
  Specifies the maximum number of rows/entities in the output result set/file. The default value is **10**, not including the total row/entity. The maximum value is **1000**.
- **measures**
  Specifies a list of measures that can be used with the chosen entity type. The options are:
  - **requests**
    The total number of requests for the selected filter (entity).

- **occurences**
  Number of occurences for the selected filter (relevant for attack-type, violation and ip-address-intelligence entities)

- **order-by**
  Specifies the measures and sort type (ascending or descending) that will be used to sort the final report. The value for each measure is a previously chosen measure. The default value for sort type is **desc** (descending).
- **range**
  Specifies the time/date range of the analytics information that you want to display. The given results will reflect the time range chosen here. The default value is the last hour (now--now-1h).
- **smtp-config-override**
  Specifies the SMTP configuration to use when sending reports by email. This overrides the default SMTP settings.

See Also

show, *save*, *send-mail*, *tmsh*, *analytics*, *analytics*, *report*

scheduled-report

Configure scheduled reports for application security (ASM).

Syntax

Configure the **scheduled-report** component within the **analytics application-security** module using the syntax shown in the following sections.

Create/Modify

```
create scheduled-report [name]
modify scheduled-report [name]
    email-addresses [none | add | delete | modify |
      replace-all-with] { email-address [string] }
    first-time [date]
    frequency [every-6-hours | every-12-hours | every-24-hours | every-week |
every-month]
    include-total [enabled | disabled]
    multi-leveled-report {
        chart-path [none | add | delete | modify | replace-all-with] { entity name
[string] }
        limit [number of rows]
        time-diff [last-hour | last-day | last-week | last-month | last-year]
        view-by { entity name [string] }
    }
    predefined-report-name [name]
    smtp-config [name]
```

Display

```
list scheduled-report
list scheduled-report [ [ [name] | [glob] | [regex] ] ... ]
show running-config scheduled-report
show running-config scheduled-report [ [ [name] | [glob] | [regex] ] ... ]
```

Delete

```
delete scheduled-report [name]
```

Description

Use the **scheduled-report** component to create, modify or delete scheduled reports for the application security module.

Examples

create scheduled-report myScheduledReport first-time now predefined-report-name "Top blocked URLs" frequency every-6-hours email-addresses add { person@domain.com } smtp-config asm_smtp_conf

Creates a scheduled report, startfroming from the next hour and executing every 6 hours. The report contains a PDF showing statistics for the top blocked URLs and is sent to person@domain.com using the smtp configuration defined in asm_smtp_conf.

modify scheduled-report myScheduledReport smtp-config none

Set smtp configuration of the scheduled report "myScheduledReport" to none, thus effectively disabling the scheduled report from begin generated and sent over eMail.

create scheduled-report myCustomScheduledReport first-time now email-addresses add { person@domain.com } frequency every-6-hours smtp-config asm_smtp_conf multi-leveled-report { view-by url time-diff last-hour limit 5 chart-path add { policy violation } }

Creates a scheduled report, starting from the next hour and executing every 6 hours. The report contains a PDF showing statistics for the top 5 violated URLs after drilling-down to the top policy followed by the top violation.
The report is sent to person@domain.co using the smtp configuration defined in asm_smtp_conf.

list scheduled-report

Displays all of the application security scheduled reports.

Options

- **email-addresses**
  A list of the email addresses of the recipients that receive the scheduled report.
- **first-time**
  First scheduled report time. Must be after current time and rounded up to the next round hour.
- **frequency**
  The scheduled report frequency. Example: every-6-hours means that the report will be generated and sent every 6 hours.
- **include-total**
  Enables or disables including a summary (Overall result) entity in results.
- **multi-leveled-report**
  Defines a custom multi-leveled report. Mutually exclusive with predefined-report-name. The **multi-leveled-report** definition contains the following parameters:

- **chart-path**
  A list of entities that define the scope in which the report will be diplayed. For example: a chart path { violation url } means: Use the top violation list and generate a top URL list from it. These top URLs will be then used to display the view-by entity. For a list of valid entities see the help manual for **analytics application-security report**.
- **limit**
  The number of **view-by** entities displayed in the scheduled report.
- **time-diff**
  The time range for the report.
- **view-by**
  The main entity that the report is viewed by. For a list of valid entities see the help manual for **analytics application-security report**.

◆ **predefined-report-name**
Defines which predefined report (AKA predefined filter) will be used to generate the report. This keyword is mutually exclusive with multi-leveled-report.

◆ **smtp-config**
Defines which SMTP configuration will be used to send the scheduled report. If set to **none**, the scheduled report will be disabled.

See Also

list, *modify*, *show*, *tmsh*, *report*, *smtp-server*

6

analytics application-security-network

- Introducing the analytics application-security-network module
- Alphabetical list of components

Introducing the analytics application-security-network module

You can use the tmsh components that reside within the analytics application-security-network module to generate analytics reports.

For more information about the tmsh hierarchical structure, see Chapter 2, *Understanding and Using the Traffic Management Shell*.

Alphabetical list of components

The remainder of this chapter lists the tmsh components that are available in the analytics application-security-network module.

report

Displays an application-security-network analytics report.

Syntax

Show, save or send an **analytics application-security report** using the syntax shown in the following sections.

Display

```
show report view-by [ application | virtual | request-type | policy ]
  drilldown {
    {
        entity [ application | virtual | request-type | policy ]
        values
        {
          [value ...]
        }
    } ...
  }
  field-fmt
  include-total
  include-others
  limit [number of rows]
  measures {
    [measure name ...]
  }
  order-by {
    {
      measure [ measure name ]
      sort-type [ asc / desc ]
    } ...
  }
  range [date range]
```

Save

```
save report view-by [ application | virtual | request-type | policy ]
   drilldown {
    {
        entity [ application | virtual | request-type | policy ]
        values
        {
          [value ...]
        }
    } ...
  }
  file [ file name ]
  format [ csv-aggregated | csv-time-series | pdf ]
  include-total
  include-others
  limit [number of rows]
  measures {
    [measure name ...]
  }
  order-by {
```

```
    {
      measure [ measure name ]
      sort-type [ asc / desc ]
    } ...
  }
  range [date range]
```

Send

```
send-mail report view-by [ application | virtual | request-type | policy ]
  drilldown {
    {
        entity [ application | virtual | request-type | policy ]
        values
        {
          [value ...]
        }
    } ...
  }
  email-addresses {
     [email address ...]
  }
  format [ csv-aggregated | csv-time-series | pdf ]
  include-total
  include-others
  limit [number of rows]
  measures {
    [measure name ...]
  }
  order-by {
    {
      measure [ measure name ]
      sort-type [ asc / desc ]
    } ...
  }
  range [date range]
  smtp-config-override [ smtp configuration object name ]
```

Description

Use this command to generate application-security-network analytics reports. You can generate an application-security-network analytics report for the following entities:

- **application** - Application services.
- **virtual** - Virtual servers.
- **request-type** - Request types (Legal/Alarmed/Blocked).
- **policy** - Security policy.

Different measures are collected for each of these entities and can be a part of the report request.

Examples

show analytics application-security-network report view-by violation

show analytics application-security-network report view-by violation drilldown { { entity severity values { Error } } }

send-mail analytics application-security-network report view-by virtual measures {events} limit 20 order-by { { measure events sort-type desc } } format pdf email-addresses { some.one@someaddress.com }

For more syntactical examples see manual for **analytics report**.

Options

- **device**
  Specifies a BIG-IP device on which to generate a report. (Enterprise Manager only)
- **device-list**
  Specifies a custom list of BIG-IP devices on which to generate a report. (Enterprise Manager only)
- **drilldown**
  Specifies specific entities that are used as a filter.
- **email-addresses**
  Specifies the list of email addresses to which the report file is sent when using the **send-mail** command.
- **file**
  Specifies the exported file path to be saved when using the **save** command. The file name should be simple (not a full path).
- **format**
  Specifies the exported file format to be saved or sent. This option must be specified when using the **save** or **send-mail** commands.
- **include-others**
  Specifies that the grand total for the measure is displayed for all entities, except for those shown in the result. It can be used along with **include-total**.
- **include-total**
  Specifies that a total summary row should be added to the analytics report. For average measures, the total value is also an average.
- **limit**
  Specifies the maximum number of rows/entities in the output result set/file. The default value is **10**, not including the total row/entity. The maximum value is **1000**.
- **measures**
  Specifies a list of measures that can be used with the chosen entity type. The options are:
  - **events**
    The total number of events (requests) for the selected filter (entity).

  - **throughput**
    The average throughput (bits/s) for the selected filter (entity).
  - **tps**
    The average number of transactions per second for the selected filter (entity).
- **order-by**
  Specifies the measures and sort type (ascending or descending) that will be used to sort the final report. The value for each measure is a previously chosen measure. The default value for sort type is **desc** (descending).
- **range**
  Specifies the time/date range of the analytics information that you want to display. The given results will reflect the time range chosen here. The default value is the last hour (now--now-1h).
- **smtp-config-override**
  Specifies the SMTP configuration to use when sending reports by email. This overrides the default SMTP settings.

See Also

show, *save*, *send-mail*, *tmsh*, *analytics*, *analytics*, *report*

7

analytics application-security-anomalies

- Introducing the analytics application-security-anomalies module
- Alphabetical list of components

Introducing the analytics application-security-anomalies module

You can use the tmsh components that reside within the analytics application-security-anomalies module to generate analytics reports.

For more information about the tmsh hierarchical structure, see Chapter 2, *Understanding and Using the Traffic Management Shell*.

Alphabetical list of components

The remainder of this chapter lists the tmsh components that are available in the analytics application-security-anomalies module.

report

Displays an application-security-anomalies analytics report.

Syntax

Show, save or send an **analytics application-security-anomalies report** using the syntax shown in the following sections.

Display

```
show report view-by [ anomaly-type | application | policy | virtual ]
  drilldown {
    {
        entity [ anomaly-type | application | policy | virtual ]
        values
        {
          [value ...]
        }
    } ...
  }
  field-fmt
  include-total
  include-others
  limit [number of rows]
  measures {
    [measure name ...]
  }
  order-by {
    {
      measure [ measure name ]
      sort-type [ asc / desc ]
    } ...
  }
  range [date range]
```

Save

```
save report view-by [ anomaly-type | application | policy | virtual ]
   drilldown {
    {
        entity [ anomaly-type | application | policy | virtual ]
        values
        {
          [value ...]
        }
    } ...
  }
  file [ file name ]
  format [ csv-aggregated | csv-time-series | pdf ]
  include-total
  include-others
  limit [number of rows]
  measures {
    [measure name ...]
  }
  order-by {
```

```
    {
      measure [ measure name ]
      sort-type [ asc / desc ]
    } ...
  }
  range [date range]
```

Send

```
send-mail report view-by [ anomaly-type | application | policy | virtual ]
  drilldown {
    {
        entity [ anomaly-type | application | policy | virtual ]
        values
        {
          [value ...]
        }
    } ...
  }
  email-addresses {
     [email address ...]
  }
  format [ csv-aggregated | csv-time-series | pdf ]
  include-total
  include-others
  limit [number of rows]
  measures {
    [measure name ...]
  }
  order-by {
    {
      measure [ measure name ]
      sort-type [ asc / desc ]
    } ...
  }
  range [date range]
  smtp-config-override [ smtp configuration object name ]
```

Description

Use this command to generate application-security-anomalies analytics reports. You can generate an application-security-network analytics report for the following entities:

- **anomaly-type** - Anomaly type (Brute Force/Web Scraping)
- **application** - Application services.
- **policy** - Security policy.
- **virtual** - Virtual servers.

Different measures are collected for each of these entities and can be a part of the report request.

Examples

show analytics application-security-network report view-by application

show analytics application-security-network report view-by application drilldown { { entity virtual values { my_vip } } }

send-mail analytics application-security-anomalies report view-by virtual measures { rejected-requests } limit 20 order-by { { measure rejected-requests sort-type desc } } format pdf email-addresses { some.one@someaddress.com }

For more syntactical examples, see the tmsh help manual for **analytics report**.

Options

- **device**
  Specifies a BIG-IP device on which to generate a report. (Enterprise Manager only)
- **device-list**
  Specifies a custom list of BIG-IP devices on which to generate a report. (Enterprise Manager only)
- **drilldown**
  Specifies specific entities that are used as a filter.
- **email-addresses**
  Specifies the list of email addresses to which the report file is sent when using the **send-mail** command.
- **file**
  Specifies the exported file path to be saved when using the **save** command. The file name should be simple (not a full path).
- **format**
  Specifies the exported file format to be saved or sent. This option must be specified when using the **save** or **send-mail** commands.
- **include-others**
  Specifies that the grand total for the measure is displayed for all entities, except for those shown in the result. It can be used along with **include-total**.
- **include-total**
  Specifies that a total summary row should be added to the analytics report. For average measures, the total value is also an average.
- **limit**
  Specifies the maximum number of rows/entities in the output result set/file. The default value is **10**, not including the total row/entity. The maximum value is **1000**.
- **measures**
  Specifies a list of measures that can be used with the chosen entity type. The options are:

  - **rejected-requests**
    The total number of rejected requests for the selected filter (entity).
  - **total-attacks**
    The total number of attacks for the selected filter (entity).
  - **total-violations**
    The total number of violations for the selected filter (entity).
- **order-by**
  Specifies the measures and sort type (ascending or descending) that will be used to sort the final report. The value for each measure is a previously chosen measure. The default value for sort type is **desc** (descending).
- **range**
  Specifies the time/date range of the analytics information that you want to display. The given results will reflect the time range chosen here. The default value is the last hour (now--now-1h).
- **smtp-config-override**
  Specifies the SMTP configuration to use when sending reports by email. This overrides the default SMTP settings.

See Also

show, *save*, *send-mail*, *tmsh*, *analytics*, *analytics*, *report*

8

analytics cpu

- Introducing the analytics cpu module
- Alphabetical list of components

Introducing the analytics cpu module

You can use the tmsh components that reside within the analytics CPU module to generate analytics reports. For more information about the tmsh hierarchical structure, see Chapter 2, *Understanding and Using the Traffic Management Shell*.

Alphabetical list of components

The remainder of this chapter lists the tmsh components that are available in the analytics CPU module.

report

Displays an cpu analytics report.

Syntax

Show, save or send an **analytics cpu report** using the syntax shown in the following sections.

Display

```
show report view-by [ slot | cpu ]
  drilldown {
    {
        entity [ slot | cpu ]
        values
        {
          [value ...]
        }
    } ...
  }
  field-fmt
  include-total
  include-others
  limit [number of rows]
  measures {
    [measure name ...]
  }
  order-by {
    {
      measure [ measure name ]
      sort-type [ asc / desc ]
    } ...
  }
  range [date range]
```

Save

```
save report view-by [ slot | cpu ]
   drilldown {
    {
        entity [ slot | cpu ]
        values
        {
          [value ...]
        }
    } ...
  }
  file [ file name ]
  format [ csv-aggregated | csv-time-series | pdf ]
  include-total
  include-others
  limit [number of rows]
  measures {
    [measure name ...]
  }
  order-by {
```

```
    {
      measure [ measure name ]
      sort-type [ asc / desc ]
    } ...
  }
  range [date range]
```

Send

```
send-mail report view-by [ slot | cpu ]
  drilldown {
    {
        entity [ slot | cpu ]
        values
        {
          [value ...]
        }
    } ...
  }
  email-addresses {
     [email address ...]
  }
  format [ csv-aggregated | csv-time-series | pdf ]
  include-total
  include-others
  limit [number of rows]
  measures {
    [measure name ...]
  }
  order-by {
    {
      measure [ measure name ]
      sort-type [ asc / desc ]
    } ...
  }
  range [date range]
  smtp-config-override [ smtp configuration object name ]
```

Description

Use this command to generate cpu analytics reports. You can generate a IP-layer analytics report for the following entities:

- **slot** - Slot ID
- **cpu** - CPU number ID

Different measures are collected for each of these entities and can be a part of the report request.

Examples

show analytics cpu report view-by cpu

show analytics cpu report view-by cpu drilldown { { entity cpu values { 1 } } }

send-mail analytics cpu report view-by slot measures { cpu-usage } limit 20 order-by { { measure cpu-usage sort-type desc } } format pdf email-addresses { some.one@someaddress.com }

For more syntactical examples, see the tmsh help manual for **analytics report**.

Options

- **device**
  Specifies a BIG-IP device on which to generate a report. (Enterprise Manager only)
- **device-list**
  Specifies a custom list of BIG-IP devices on which to generate a report. (Enterprise Manager only)
- **drilldown**
  Specifies specific entities that are used as a filter.
- **email-addresses**
  Specifies the list of email addresses to which the report file is sent when using the **send-mail** command.
- **file**
  Specifies the exported file path to be saved when using the **save** command. The file name should be simple (not a full path).
- **format**
  Specifies the exported file format to be saved or sent. This option must be specified when using the **save** or **send-mail** commands.
- **include-others**
  Specifies that the grand total for the measure is displayed for all entities, except for those shown in the result. It can be used along with **include-total**.
- **include-total**
  Specifies that a total summary row should be added to the analytics report. For average measures, the total value is also an average.
- **limit**
  Specifies the maximum number of rows/entities in the output result set/file. The default value is **10**, not including the total row/entity. The maximum value is **1000**.
- **measures**
  Specifies a list of measures that can be used with the chosen entity type. The options are:
  - **cpu-usage**
    The average time percentage of real CPU usage (user + system + nice) usage for the selected filter (entity).

  - **io**
    The average time percentage of (iowait + irq + softirq) for the selected filter (entity).
  - **stolen**
    The average time percentage of virtual CPU waits for a real CPU while the hypervisor is servicing another virtual processor.

- **order-by**
  Specifies the measures and sort type (ascending or descending) that will be used to sort the final report. The value for each measure is a previously chosen measure. The default value for sort type is **desc** (descending).
- **range**
  Specifies the time/date range of the analytics information that you want to display. The given results will reflect the time range chosen here. The default value is the last hour (now--now-1h).
- **smtp-config-override**
  Specifies the SMTP configuration to use when sending reports by email. This overrides the default SMTP settings.

See Also

show, *save*, *send-mail*, *tmsh*, *analytics*, *analytics*, *report*

9

analytics disk-info

- Introducing the analytics disk-info module
- Alphabetical list of components

Introducing the analytics disk-info module

You can use the tmsh components that reside within the analytics disk-info module to generate analytics reports. For more information about the tmsh hierarchical structure, see Chapter 2, *Understanding and Using the Traffic Management Shell*.

Alphabetical list of components

The remainder of this chapter lists the tmsh components that are available in the analytics disk-info module.

report

Displays an disk-info analytics report.

Syntax

Show, save or send an **analytics disk-info report** using the syntax shown in the following sections.

Display

```
show report view-by [ slot ]
  drilldown {
    {
        entity [ slot ]
        values
        {
          [value ...]
        }
    } ...
  }
  field-fmt
  include-total
  include-others
  limit [number of rows]
  measures {
    [measure name ...]
  }
  order-by {
    {
      measure [ measure name ]
      sort-type [ asc / desc ]
    } ...
  }
  range [date range]
```

Save

```
save report view-by [ slot ]
   drilldown {
    {
        entity [ slot ]
        values
        {
          [value ...]
        }
    } ...
  }
  file [ file name ]
  format [ csv-aggregated | csv-time-series | pdf ]
  include-total
  include-others
  limit [number of rows]
  measures {
    [measure name ...]
  }
  order-by {
```

```
    {
      measure [ measure name ]
      sort-type [ asc / desc ]
    } ...
  }
  range [date range]
```

Send

```
send-mail report view-by [ slot ]
  drilldown {
    {
        entity [ slot ]
        values
        {
          [value ...]
        }
    } ...
  }
  email-addresses {
     [email address ...]
  }
  format [ csv-aggregated | csv-time-series | pdf ]
  include-total
  include-others
  limit [number of rows]
  measures {
    [measure name ...]
  }
  order-by {
    {
      measure [ measure name ]
      sort-type [ asc / desc ]
    } ...
  }
  range [date range]
  smtp-config-override [ smtp configuration object name ]
```

Description

Use this command to generate disk-info analytics reports. You can generate a disk-info analytics report for the following entities:

- **slot** - Slot ID

Different measures are collected for each of these entities and can be a part of the report request.

Examples

show analytics disk-info report view-by slot

show analytics disk-info report view-by slot drilldown { { entity slot values { 7 } } }

send-mail analytics disk-info report view-by slot measures { total-ios } limit 20 order-by { { measure total-ios sort-type desc } } format pdf email-addresses { some.one@someaddress.com }

For more syntactical examples, see the tmsh help manual for **analytics report**.

Options

- **device**
  Specifies a BIG-IP device on which to generate a report. (Enterprise Manager only)
- **device-list**
  Specifies a custom list of BIG-IP devices on which to generate a report. (Enterprise Manager only)
- **drilldown**
  Specifies specific entities that are used as a filter.
- **email-addresses**
  Specifies the list of email addresses to which the report file is sent when using the **send-mail** command.
- **file**
  Specifies the exported file path to be saved when using the **save** command. The file name should be simple (not a full path).
- **format**
  Specifies the exported file format to be saved or sent. This option must be specified when using the **save** or **send-mail** commands.
- **include-others**
  Specifies that the grand total for the measure is displayed for all entities, except for those shown in the result. It can be used along with **include-total**.
- **include-total**
  Specifies that a total summary row should be added to the analytics report. For average measures, the total value is also an average.
- **limit**
  Specifies the maximum number of rows/entities in the output result set/file. The default value is **10**, not including the total row/entity. The maximum value is **1000**.
- **measures**
  Specifies a list of measures that can be used with the chosen entity type. The options are:
  - **total-ios**
    The total number of I/O for the selected filter (entity).
  - **read-operations**
    The total number of read operations for the selected filter (entity).
  - **read-merged**
    The total number of merged reads for the selected filter (entity).

- **write-operations**
  The total number of write operations for the selected filter (entity).
- **write-merged**
  The total number of merged writes for the selected filter (entity).
- **read-bytes**
  The total number of read bytes for the selected filter (entity).
- **write-bytes**
  The total number of write bytes for the selected filter (entity).
- **max-read-latency**
  The max value of read latency for the selected filter (entity).
- **average-read-latency**
  The average number of average read latency for the selected filter (entity).

◆ **order-by**
Specifies the measures and sort type (ascending or descending) that will be used to sort the final report. The value for each measure is a previously chosen measure. The default value for sort type is **desc** (descending).

◆ **range**
Specifies the time/date range of the analytics information that you want to display. The given results will reflect the time range chosen here. The default value is the last hour (now--now-1h).

◆ **smtp-config-override**
Specifies the SMTP configuration to use when sending reports by email. This overrides the default SMTP settings.

See Also

show, *save*, *send-mail*, *tmsh*, *analytics*, *analytics*, *report*

10

analytics dns

- Introducing the analytics dns module
- Alphabetical list of components

Introducing the analytics dns module

You can use the tmsh components that reside within the analytics DNS module to generate analytics reports. For more information about the tmsh hierarchical structure, see Chapter 2, *Understanding and Using the Traffic Management Shell*.

Alphabetical list of components

The remainder of this chapter lists the tmsh components that are available in the analytics DNS module.

report

Displays a DNS analytics report.

Syntax

Show, save or send an **analytics dns report** using the syntax shown in the following sections.

Display

```
show report view-by [ application | client-ip | domain-name | query-type | virtual ]
  drilldown {
    {
        entity [ application | client-ip | domain-name | query-type | virtual ]
        values
        {
          [value ...]
        }
    } ...
  }
  field-fmt
  include-total
  include-others
  limit [number of rows]
  measures {
    [measure name ...]
  }
  order-by {
    {
      measure [ measure name ]
      sort-type [ asc | desc ]
    } ...
  }
  range [date range]
```

Save

```
save report view-by [ application | client-ip | domain-name | query-type | virtual  ]
   drilldown {
    {
        entity [ application | client-ip | domain-name | query-type | virtual ]
        values
        {
          [value ...]
        }
    } ...
  }
  file [ file name ]
  format [ csv-aggregated | csv-time-series | pdf ]
  include-total
  include-others
  limit [number of rows]
  measures {
    [measure name ...]
  }
  order-by {
```

```
    {
      measure [ measure name ]
      sort-type [ asc | desc ]
    } ...
  }
  range [date range]
```

Send

```
send-mail report view-by [ application | client-ip | domain-name | query-type |
virtual  ]
  drilldown {
    {
        entity [ application | client-ip | domain-name | query-type | virtual ]
        values
        {
          [value ...]
        }
    } ...
  }
  email-addresses {
     [email address ...]
  }
  format [ csv-aggregated | csv-time-series | pdf ]
  include-total
  include-others
  limit [number of rows]
  measures {
    [measure name ...]
  }
  order-by {
    {
      measure [ measure name ]
      sort-type [ asc | desc ]
    } ...
  }
  range [date range]
  smtp-config-override [ smtp configuration object name ]
```

Description

Use this command to generate DNS analytics reports. You can generate a DNS analytics report for the following entities:

- **application** - Application services (iApps™).
- **client-ip** - DNS query source/client IP address.
- **domain-name** - Queried domain name.
- **query-type** - DNS query type.
- **virtual** - Virtual server.

Examples

show analytics dns report view-by virtual

show analytics dns report view-by query-type drilldown { { entity virtual values { /Common/v1 } } }

send-mail analytics dns report view-by client-ip limit 20 format pdf email-addresses { some.one@someaddress.com }

For more syntactical examples see manual for **analytics report**.

Options

- **device**
  Specifies a BIG-IP device on which to generate a report. (Enterprise Manager only)
- **device-list**
  Specifies a custom list of BIG-IP devices on which to generate a report. (Enterprise Manager only)
- **drilldown**
  Specifies specific entities that are used as a filter.
- **email-addresses**
  Specifies the list of email addresses to which the report file is sent when using the **send-mail** command.
- **file**
  Specifies the exported file path to be saved when using the **save** command. The file name should be simple (not a full path).
- **format**
  Specifies the exported file format to be saved or sent. This option must be specified when using the **save** or **send-mail** commands.
- **include-others**
  Specifies that the grand total for the measure is displayed for all entities, except for those shown in the result. It can be used along with **include-total**.
- **include-total**
  Specifies that a total summary row should be added to the analytics report. For average measures, the total value is also an average.
- **limit**
  Specifies the maximum number of rows/entities in the output result set/file. The default value is **10**, not including the total row/entity. The maximum value is **1000**.
- **measures**
  Specifies a list of measures that can be used with the chosen entity type. The options are:
  - **packets**
    The total number of DNS packets for the specified view-by entity.

- **order-by**
  Specifies the measures and sort type (ascending or descending) that will be used to sort the final report. The value for each measure is a previously chosen measure. The default value for sort type is **desc** (descending).
- **range**
  Specifies the time/date range of the analytics information that you want to display. The given results will reflect the time range chosen here. The default value is the last hour (now--now-1h).
- **smtp-config-override**
  Specifies the SMTP configuration to use when sending reports by email. This overrides the default SMTP settings.

See Also

show, *save*, *send-mail*, *tmsh*, *dns*, *analytics*, *report*

11

analytics dns-dos

- Introducing the analytics dns-dos module
- Alphabetical list of components

Introducing the analytics dns-dos module

You can use the tmsh components that reside within the analytics DNS-DoS module to generate analytics reports. For more information about the tmsh hierarchical structure, see Chapter 2, *Understanding and Using the Traffic Management Shell*.

Alphabetical list of components

The remainder of this chapter lists the tmsh components that are available in the analytics DNS-DoS module.

report

Displays a DNS DoS prevention analytics report.

Syntax

Show, save or send an **analytics dns-dos report** using the syntax shown in the following sections.

Display

```
show report view-by [ application | attack-id | attack-type | client-ip | domain-name
| query-type | virtual ]
  drilldown {
    {
        entity [ application | attack-id | attack-type | client-ip | domain-name |
query-type | virtual ]
        values
        {
          [value ...]
        }
    } ...
  }
  field-fmt
  include-total
  include-others
  limit [number of rows]
  measures {
    [measure name ...]
  }
  order-by {
    {
      measure [ measure name ]
      sort-type [ asc | desc ]
    } ...
  }
  range [date range]
```

Save

```
save report view-by [ application | attack-id | attack-type | client-ip | domain-name
| query-type | virtual ]
   drilldown {
    {
        entity [ application | attack-id | attack-type | client-ip | domain-name |
query-type | virtual ]
        values
        {
          [value ...]
        }
    } ...
  }
  file [ file name ]
  format [ csv-aggregated | csv-time-series | pdf ]
  include-total
  include-others
  limit [number of rows]
```

```
  measures {
    [measure name ...]
  }
  order-by {
    {
      measure [ measure name ]
      sort-type [ asc | desc ]
    } ...
  }
  range [date range]
```

Send

```
send-mail report view-by [ application | attack-id | attack-type | client-ip |
domain-name | query-type | virtual ]
  drilldown {
    {
        entity [ application | attack-id | attack-type | client-ip | domain-name |
query-type | virtual ]
        values
        {
          [value ...]
        }
    } ...
  }
  email-addresses {
     [email address ...]
  }
  format [ csv-aggregated | csv-time-series | pdf ]
  include-total
  include-others
  limit [number of rows]
  measures {
    [measure name ...]
  }
  order-by {
    {
      measure [ measure name ]
      sort-type [ asc | desc ]
    } ...
  }
  range [date range]
  smtp-config-override [ smtp configuration object name ]
```

Description

Use this command to generate DNS DoS prevention analytics reports. You can generate a DNS DoS prevention analytics report for the following entities:

- **application** - Application services (iApps™).
- **attack-id** - DNS DoS attack ID.
- **attack-type** - DNS DoS attack type.

- **client-ip** - DNS query source/client IP address.
- **domain-name** - Queried domain name.
- **query-type** - DNS query type.
- **virtual** - Virtual server.

Examples

show analytics dns-dos report view-by virtual

show analytics dns-dos report view-by attack-type drilldown { { entity virtual values { /Common/v1 } } { entity query-type values { A } } }

send-mail analytics dns-dos report view-by client-ip limit 20 format pdf email-addresses { some.one@someaddress.com }

For more syntactical examples see manual for **analytics report**.

Options

- **device**
  Specifies a BIG-IP device on which to generate a report. (Enterprise Manager only)
- **device-list**
  Specifies a custom list of BIG-IP devices on which to generate a report. (Enterprise Manager only)
- **drilldown**
  Specifies specific entities that are used as a filter.
- **email-addresses**
  Specifies the list of email addresses to which the report file is sent when using the **send-mail** command.
- **file**
  Specifies the exported file path to be saved when using the **save** command. The file name should be simple (not a full path).
- **format**
  Specifies the exported file format to be saved or sent. This option must be specified when using the **save** or **send-mail** commands.
- **include-others**
  Specifies that the grand total for the measure is displayed for all entities, except for those shown in the result. It can be used along with **include-total**.
- **include-total**
  Specifies that a total summary row should be added to the analytics report. For average measures, the total value is also an average.

- **limit**
  Specifies the maximum number of rows/entities in the output result set/file. The default value is **10**, not including the total row/entity. The maximum value is **1000**.
- **measures**
  Specifies a list of measures that can be used with the chosen entity type. The options are:
  - **filtered-drops**
    The total number of filtered DNS packets for the specified view-by entity.
- **order-by**
  Specifies the measures and sort type (ascending or descending) that will be used to sort the final report. The value for each measure is a previously chosen measure. The default value for sort type is **desc** (descending).
- **range**
  Specifies the time/date range of the analytics information that you want to display. The given results will reflect the time range chosen here. The default value is the last hour (now--now-1h).
- **smtp-config-override**
  Specifies the SMTP configuration to use when sending reports by email. This overrides the default SMTP settings.

See Also

show, *save*, *send-mail*, *tmsh*, *dns*, *analytics*, *report*

12

analytics dns-protocol

- Introducing the analytics dns-protocol module
- Alphabetical list of components

Introducing the analytics dns-protocol module

You can use the tmsh components that reside within the analytics DNS-protocol module to generate analytics reports. For more information about the tmsh hierarchical structure, see Chapter 2, *Understanding and Using the Traffic Management Shell*.

Alphabetical list of components

The remainder of this chapter lists the tmsh components that are available in the analytics DNS-protocol module.

report

Displays a DNS protocol security analytics report.

Syntax

Show, save or send an **analytics dns-protocol report** using the syntax shown in the following sections.

Display

```
show report view-by [ application | client-ip | domain-name | error-type | query-type
| virtual ]
  drilldown {
    {
        entity [ application | client-ip | domain-name | error-type | query-type |
virtual ]
        values
        {
          [value ...]
        }
    } ...
  }
  field-fmt
  include-total
  include-others
  limit [number of rows]
  measures {
    [measure name ...]
  }
  order-by {
    {
      measure [ measure name ]
      sort-type [ asc | desc ]
    } ...
  }
  range [date range]
```

Save

```
save report view-by [ application | client-ip | domain-name | error-type | query-type
| virtual ]
   drilldown {
    {
        entity [ application | client-ip | domain-name | error-type | query-type |
virtual ]
        values
        {
          [value ...]
        }
    } ...
  }
  file [ file name ]
  format [ csv-aggregated | csv-time-series | pdf ]
  include-total
  include-others
  limit [number of rows]
```

```
  measures {
    [measure name ...]
  }
  order-by {
    {
      measure [ measure name ]
      sort-type [ asc | desc ]
    } ...
  }
  range [date range]
```

Send

```
send-mail report view-by [ application | client-ip | domain-name | error-type |
query-type | virtual ]
  drilldown {
    {
        entity [ application | client-ip | domain-name | error-type | query-type |
virtual ]
        values
        {
          [value ...]
        }
    } ...
  }
  email-addresses {
     [email address ...]
  }
  format [ csv-aggregated | csv-time-series | pdf ]
  include-total
  include-others
  limit [number of rows]
  measures {
    [measure name ...]
  }
  order-by {
    {
      measure [ measure name ]
      sort-type [ asc | desc ]
    } ...
  }
  range [date range]
  smtp-config-override [ smtp configuration object name ]
```

Description

Use this command to generate DNS protocol security analytics reports. You can generate a DNS protocol security analytics report for the following entities:

- **application** - Application services (iApps™).
- **client-ip** - DNS query source/client IP address.
- **domain-name** - Queried domain name.

- **query-type** - DNS query type.
- **error-type** - DNS filtering error type.
- **virtual** - Virtual server.

Examples

show analytics dns-protocol report view-by virtual

show analytics dns-protocol report view-by error-type drilldown { { entity virtual values { /Common/v1 } } { entity query-type values { A } } }

send-mail analytics dns-protocol report view-by client-ip limit 20 format pdf email-addresses { some.one@someaddress.com }

For more syntactical examples see manual for **analytics report**.

Options

- **device**
  Specifies a BIG-IP device on which to generate a report. (Enterprise Manager only)
- **device-list**
  Specifies a custom list of BIG-IP devices on which to generate a report. (Enterprise Manager only)
- **drilldown**
  Specifies specific entities that are used as a filter.
- **email-addresses**
  Specifies the list of email addresses to which the report file is sent when using the **send-mail** command.
- **file**
  Specifies the exported file path to be saved when using the **save** command. The file name should be simple (not a full path).
- **format**
  Specifies the exported file format to be saved or sent. This option must be specified when using the **save** or **send-mail** commands.
- **include-others**
  Specifies that the grand total for the measure is displayed for all entities, except for those shown in the result. It can be used along with **include-total**.
- **include-total**
  Specifies that a total summary row should be added to the analytics report. For average measures, the total value is also an average.

- **limit**
  Specifies the maximum number of rows/entities in the output result set/file. The default value is **10**, not including the total row/entity. The maximum value is **1000**.
- **measures**
  Specifies a list of measures that can be used with the chosen entity type. The options are:
  - **dropped-packets**
    The total number of dropped DNS packets for the specified view-by entity.
- **order-by**
  Specifies the measures and sort type (ascending or descending) that will be used to sort the final report. The value for each measure is a previously chosen measure. The default value for sort type is **desc** (descending).
- **range**
  Specifies the time/date range of the analytics information that you want to display. The given results will reflect the time range chosen here. The default value is the last hour (now--now-1h).
- **smtp-config-override**
  Specifies the SMTP configuration to use when sending reports by email. This overrides the default SMTP settings.

See Also

show, *save*, *send-mail*, *tmsh*, *dns*, *analytics*, *report*

13

analytics dos-l3

- Introducing the analytics dos-l3 module
- Alphabetical list of components

Introducing the analytics dos-l3 module

You can use the tmsh components that reside within the analytics Denial of Servive Layer 3 (DoS l3) module to generate analytics reports. For more information about the tmsh hierarchical structure, see Chapter 2, *Understanding and Using the Traffic Management Shell*.

Alphabetical list of components

The remainder of this chapter lists the tmsh components that are available in the analytics DoS l3 module.

report

Displays a DoS (Layers 3-4) prevention analytics report.

Syntax

Show, save or send an **analytics dos-l3 report** using the syntax shown in the following sections.

Display

```
show report view-by [ action | application | attack-id | attack-type | source-ip |
virtual | vlan | vlan-group ]
  drilldown {
    {
       entity [ action | application | attack-id | attack-type | source-ip | virtual |
vlan | vlan-group ]
        values
        {
          [value ...]
        }
    } ...
  }
  field-fmt
  include-total
  include-others
  limit [number of rows]
  measures {
    [measure name ...]
  }
  order-by {
    {
      measure [ measure name ]
      sort-type [ asc | desc ]
    } ...
  }
  range [date range]
```

Save

```
save report view-by [ action | application | attack-id | attack-type | source-ip |
virtual | vlan | vlan-group ]
   drilldown {
    {
       entity [ action | application | attack-id | attack-type | source-ip | virtual |
vlan | vlan-group ]
        values
        {
          [value ...]
        }
    } ...
  }
  file [ file name ]
  format [ csv-aggregated | csv-time-series | pdf ]
  include-total
  include-others
  limit [number of rows]
```

```
  measures {
    [measure name ...]
  }
  order-by {
    {
      measure [ measure name ]
      sort-type [ asc | desc ]
    } ...
  }
  range [date range]
```

Send

```
send-mail report view-by [ action | application | attack-id | attack-type | source-ip
| virtual | vlan | vlan-group ]
  drilldown {
    {
        entity [ application | action | application | attack-id | attack-type |
source-ip | virtual | vlan | vlan-group ]
        values
        {
          [value ...]
        }
    } ...
  }
  email-addresses {
     [email address ...]
  }
  format [ csv-aggregated | csv-time-series | pdf ]
  include-total
  include-others
  limit [number of rows]
  measures {
    [measure name ...]
  }
  order-by {
    {
      measure [ measure name ]
      sort-type [ asc | desc ]
    } ...
  }
  range [date range]
  smtp-config-override [ smtp configuration object name ]
```

Description

Use this command to generate DoS (Layers 3-4) prevention analytics reports. You can generate a DoS prevention analytics report for the following entities:

- **action** - Action taken (allowed/dropped).
- **application** - Application services (iApps™).
- **attack-id** - DoS attack ID.

- **attack-type** - DoS attack type.
- **source-ip** - Source/client IP address.
- **virtual** - Virtual server.
- **vlan** - VLAN.
- **vlan-group** - VLAN Group.

Examples

show analytics dos-l3 report view-by virtual

show analytics dos-l3 report view-by attack-type drilldown { { entity virtual values { /Common/v1 } } }

send-mail analytics dos-l3 report view-by source-ip limit 20 format pdf email-addresses { some.one@someaddress.com }

For more syntactical examples see manual for **analytics report**.

Options

- **device**
  Specifies a BIG-IP device on which to generate a report. (Enterprise Manager only)
- **device-list**
  Specifies a custom list of BIG-IP devices on which to generate a report. (Enterprise Manager only)
- **drilldown**
  Specifies specific entities that are used as a filter.
- **email-addresses**
  Specifies the list of email addresses to which the report file is sent when using the **send-mail** command.
- **file**
  Specifies the exported file path to be saved when using the **save** command. The file name should be simple (not a full path).
- **format**
  Specifies the exported file format to be saved or sent. This option must be specified when using the **save** or **send-mail** commands.
- **include-others**
  Specifies that the grand total for the measure is displayed for all entities, except for those shown in the result. It can be used along with **include-total**.

- **include-total**
  Specifies that a total summary row should be added to the analytics report. For average measures, the total value is also an average.
- **limit**
  Specifies the maximum number of rows/entities in the output result set/file. The default value is **10**, not including the total row/entity. The maximum value is **1000**.
- **measures**
  Specifies a list of measures that can be used with the chosen entity type. The options are:
  - **allowed-requests**
    The total number of packets that were recieved by the virtual server(/s)s
  - **dropped-requests**
    The total number of packets that were dropped by the virtual server(/s)s
  - **total-requests**
    The total number of packets that were recieved or dropped by the virtual server(/s)s
- **order-by**
  Specifies the measures and sort type (ascending or descending) that will be used to sort the final report. The value for each measure is a previously chosen measure. The default value for sort type is **desc** (descending).
- **range**
  Specifies the time/date range of the analytics information that you want to display. The given results will reflect the time range chosen here. The default value is the last hour (now--now-1h).
- **smtp-config-override**
  Specifies the SMTP configuration to use when sending reports by email. This overrides the default SMTP settings.

See Also

show, *save*, *send-mail*, *tmsh*, *analytics*, *report*

14

analytics dos-l7

- Introducing the analytics dos-l7 module
- Alphabetical list of components

Introducing the analytics dos-l7 module

You can use the tmsh components that reside within the analytics Denial of Servive Layer 7 (DoS l7) module to generate analytics reports. For more information about the tmsh hierarchical structure, see Chapter 2, *Understanding and Using the Traffic Management Shell*.

Alphabetical list of components

The remainder of this chapter lists the tmsh components that are available in the analytics DoS l7 module.

report

Displays an HTTP/L7-DoS analytics report.

Syntax

Show, save or send an **analytics dos-l7 report** using the syntax shown in the following sections.

Display

```
show report view-by [ application | virtual | pool-member | url |
                      client-ip | country | response-code |
                      method | user-agent | client-subnet |
                      dos17-attack-id | profile | transaction-outcome ]
  drilldown {
    {
        entity [ application | virtual | pool-member | url |
                 client-ip | country | response-code | method |
                 user-agent | client-subnet | dos17-attack-id |
                 profile | transaction-outcome ]
        values
        {
          [value ...]
        }
    } ...
  }
  field-fmt
  include-total
  include-others
  limit [number of rows]
  measures {
    [measure name ...]
  }
  order-by {
    {
      measure [ measure name ]
      sort-type [ asc / desc ]
    } ...
  }
  range [date range]
```

Save

```
save report view-by [ application | virtual | pool-member | url |
                      client-ip | country | response-code |
                      method | user-agent | client-subnet |
                      dos17-attack-id | profile | transaction-outcome ]
   drilldown {
    {
        entity [ application | virtual | pool-member | url |
                 client-ip | country | response-code | method |
                 user-agent | client-subnet | dos17-attack-id |
                 profile | transaction-outcome ]
        values
        {
          [value ...]
```

```
        }
    } ...
}
file [ file name ]
format [ csv-aggregated | csv-time-series | pdf ]
include-total
include-others
limit [number of rows]
measures {
  [measure name ...]
}
order-by {
  {
    measure [ measure name ]
    sort-type [ asc / desc ]
  } ...
}
range [date range]
```

Send

```
send-mail report view-by [ application | virtual | pool-member |
                           url | client-ip | country | response-code |
                           method | user-agent | client-subnet |
                           dos17-attack-id | profile | transaction-outcome ]
  drilldown {
    {
        entity [ application | virtual | pool-member | url | client-ip |
                 country | response-code | method | user-agent | client-subnet |
                 dos17-attack-id | profile | transaction-outcome ]
        values
        {
          [value ...]
        }
    } ...
  }
  email-addresses {
     [email address ...]
  }
  format [ csv-aggregated | csv-time-series | pdf ]
  include-total
  include-others
  limit [number of rows]
  measures {
    [measure name ...]
  }
  order-by {
    {
      measure [ measure name ]
      sort-type [ asc / desc ]
    } ...
  }
  range [date range]
  smtp-config-override [ smtp configuration object name ]
```

Description

Use this command to generate HTTP analytics reports. You can generate an HTTP analytics report for the following entities:

- **application** - Application services.
- **virtual** - Virtual servers.
- **pool-member** - Pool members.
- **url** - A URL accessed by HTTP or HTTPs.
- **client-ip** - A single client identified by an IP address.
- **country** - A country from which HTTP/HTTPs traffic was sent to each of the virtual servers.
- **response-code** - An HTTP response code that was sent back to the client.
- **method** - An HTTP method used by the client (GET, CREATE, POST, DELETE, etc.).
- **user-agent** - A browser identifier sent by the client's browser as part of the request for URL.
- **subnet** - Client IP addresses classified into subnets.
- **dosl7-attack-id** - Application/L7 DoS Attack ID.
- **profile** - DoS Layer 7 (Application) Profile.
- **transaction-outcome** - Transaction outcomes (Blocked/Dropped/Passthrought/etc.)

Different measures are collected for each of these entities and can be a part of the report request.

Examples

show analytics http report view-by virtual measures {average-tps} limit 20

Gets the average tps of 20 virtual servers (unordered).

show analytics http report view-by virtual measures {average-tps} limit 20 order-by { { measure average-tps sort-type desc } }

Gets the average tps of the top 20 virtual servers.

show analytics http report view-by virtual measures {average-tps} limit 20 order-by { { measure average-tps sort-type desc } } range now-3d--now

Gets the average tps of the top 20 virtual servers from the last three days.

show analytics http report view-by virtual drilldown { { entity application values { app } } { entity pool-member values { p1 p2 } } } range now-4d--now-2d measures {average-tps} limit 10 order-by { { measure average-tps sort-type DESC } }

Gets the average tps of the top 10 virtual servers (ordered by average tps) on **app** iApp (out of several monitored) on pool members **p1** and **p2**

show analytics http report view-by response-code drilldown { { entity virtual values { v1 } } } measures { transactions }

Gets a distribution of requests per response code on virtual v1.

show analytics http report view-by country drilldown { { entity application values { app } } } measures { average-concurrent-sessions average-sessions } order-by { { measure average-sessions sort-type DESC } } limit 5

Gets the new sessions and average concurrent sessions of the top five countries, ordered by the average concurrent sessions on the application **app**.

show analytics http report view-by client-ip drilldown { { entity virtual values { v1 } } } measures { max-page-load-time } limit 1

Gets the client IP address with the worst page load time.

show analytics http report view-by application drilldown { { entity pool-member values { p1 p2 } } } measures { transactions } order-by { { measure transactions } } range now-7d--now

Gets the distribution of requests per application on pool members *p1*

save analytics http report view-by virtual measures {average-tps} limit 20 order-by { { measure average-tps sort-type desc } } format pdf file report.pdf

Gets the average tps of the top 20 virtual servers and exports to a PDF file on the BIG-IP system.

save analytics http report view-by virtual measures {average-tps} limit 20 order-by { { measure average-tps sort-type desc } } format csv-aggregated file report.csv

Gets the average tps of the top 20 virtual servers and exports to a CSV file on the BIG-IP system.

save analytics http report view-by virtual measures {average-tps} limit 20 order-by { { measure average-tps sort-type desc } } format csv-time-series file report.csv

Gets the average tps over time of the top 10 virtual servers and exports to a CSV file on the BIG-IP system.

send-mail analytics http report view-by virtual measures {average-tps} limit 20 order-by { { measure average-tps sort-type desc } } format pdf email-addresses { some.one@someaddress.com }

Gets the average tps over time of the top 10 virtual servers and sends out an email containing the report as a PDF.

Options

- **device**
  Specifies a BIG-IP device on which to generate a report. (Enterprise Manager only)
- **device-list**
  Specifies a custom list of BIG-IP devices on which to generate a report. (Enterprise Manager only)
- **drilldown**
  Specifies specific entities that are used as a filter.
- **email-addresses**
  Specifies the list of email addresses to which the report file is sent when using the **send-mail** command.
- **file**
  Specifies the exported file path to be saved when using the **save** command. The file name should be simple (not a full path).
- **format**
  Specifies the exported file format to be saved or sent. This option must be specified when using the **save** or **send-mail** commands.
- **include-others**
  Specifies that the grand total for the measure is displayed for all entities, except for those shown in the result. It can be used along with **include-total**.
- **include-total**
  Specifies that a total summary row should be added to the analytics report. For average measures, the total value is also an average.
- **limit**
  Specifies the maximum number of rows/entities in the output result set/file. The default value is **10**, not including the total row/entity. The maximum value is **1000**.
- **measures**
  Specifies a list of measures that can be used with the chosen entity type. The default value is **transactions**. The options are:
  - **average-concurrent-sessions**
    The average number of concurrent sessions for each entity.
  - **average-new-sessions**
    The average number of new sessions for each entity.
  - **average-page-load-time**
    The average client page load time for each entity.
  - **average-request-throughput**
    The average request throughput for each entity.

- **average-response-throughput**
  The average response throughput for each entity.
- **average-server-latency**
  The average server latency for each entity.
- **average-tps**
  The average number of transactions per second for each entity.
- **client-side-sampled-transactions**
  The number of transactions sampled for client side page load time.
- **max-page-load-time**
  The maximum client page load time for each entity.
- **max-request-throughput**
  The maximum request throughput for each entity.
- **max-response-throughput**
  The maximum response throughput for each entity.
- **max-server-latency**
  The maximum server latency for each entity.
- **max-tps**
  The maximum number of transactions per second for each entity.
- **transactions**
  The absolute number of transactions for each entity.

◆ **order-by**
Specifies the measures and sort type (ascending or descending) that will be used to sort the final report. The default value for measures is previously chosen measures. The default value for sort type is **desc** (descending).

◆ **range**
Specifies the time/date range of the analytics information that you want to display. The given results will reflect the time range chosen here. The default value is the last hour (now--now-1h).

◆ **smtp-config-override**
Specifies the SMTP configuration to use when sending reports by email. This overrides the default SMTP settings.

See Also

show, *save*, *send-mail*, *tmsh*, *analytics*, *profile*, *report*

15

analytics http

- Introducing the analytics http module
- Alphabetical list of components

Introducing the analytics http module

You can use the tmsh components that reside within the analytics http module to generate analytics reports. For more information about the tmsh hierarchical structure, see Chapter 2, *Understanding and Using the Traffic Management Shell*.

Alphabetical list of components

The remainder of this chapter lists the tmsh components that are available in the analytics http module.

report

Displays an HTTP/L7-DoS analytics report.

Syntax

Show, save or send an **analytics http report** using the syntax shown in the following sections.

Display

```
show report view-by [ application | virtual | pool-member | url |
                      client-ip | country | response-code |
                      method | user-agent | client-subnet |
                      dos17-attack-id | profile | transaction-outcome ]
  drilldown {
    {
        entity [ application | virtual | pool-member | url |
                 client-ip | country | response-code | method |
                 user-agent | client-subnet | dos17-attack-id |
                 profile | transaction-outcome ]
        values
        {
          [value ...]
        }
    } ...
  }
  field-fmt
  include-total
  include-others
  limit [number of rows]
  measures {
    [measure name ...]
  }
  order-by {
    {
      measure [ measure name ]
      sort-type [ asc / desc ]
    } ...
  }
  range [date range]
```

Save

```
save report view-by [ application | virtual | pool-member | url |
                      client-ip | country | response-code |
                      method | user-agent | client-subnet |
                      dos17-attack-id | profile | transaction-outcome ]
   drilldown {
    {
        entity [ application | virtual | pool-member | url |
                 client-ip | country | response-code | method |
                 user-agent | client-subnet | dos17-attack-id |
                 profile | transaction-outcome ]
        values
        {
          [value ...]
```

```
        }
    } ...
}
file [ file name ]
format [ csv-aggregated | csv-time-series | pdf ]
include-total
include-others
limit [number of rows]
measures {
  [measure name ...]
}
order-by {
  {
    measure [ measure name ]
    sort-type [ asc / desc ]
  } ...
}
range [date range]
```

Send

```
send-mail report view-by [ application | virtual | pool-member |
                           url | client-ip | country | response-code |
                           method | user-agent | client-subnet |
                           dos17-attack-id | profile | transaction-outcome ]
  drilldown {
    {
        entity [ application | virtual | pool-member | url | client-ip |
                 country | response-code | method | user-agent | client-subnet |
                 dos17-attack-id | profile | transaction-outcome ]
        values
        {
          [value ...]
        }
    } ...
  }
  email-addresses {
     [email address ...]
  }
  format [ csv-aggregated | csv-time-series | pdf ]
  include-total
  include-others
  limit [number of rows]
  measures {
    [measure name ...]
  }
  order-by {
    {
      measure [ measure name ]
      sort-type [ asc / desc ]
    } ...
  }
  range [date range]
  smtp-config-override [ smtp configuration object name ]
```

Description

Use this command to generate HTTP analytics reports. You can generate an HTTP analytics report for the following entities:

- **application** - Application services.
- **virtual** - Virtual servers.
- **pool-member** - Pool members.
- **url** - A URL accessed by HTTP or HTTPs.
- **client-ip** - A single client identified by an IP address.
- **country** - A country from which HTTP/HTTPs traffic was sent to each of the virtual servers.
- **response-code** - An HTTP response code that was sent back to the client.
- **method** - An HTTP method used by the client (GET, CREATE, POST, DELETE, etc.).
- **user-agent** - A browser identifier sent by the client's browser as part of the request for URL.
- **subnet** - Client IP addresses classified into subnets.
- **dosl7-attack-id** - Application/L7 DoS Attack ID.
- **profile** - DoS Layer 7 (Application) Profile.
- **transaction-outcome** - Transaction outcomes (Blocked/Dropped/Passthrought/etc.)

Different measures are collected for each of these entities and can be a part of the report request.

Examples

show analytics http report view-by virtual measures {average-tps} limit 20

Gets the average tps of 20 virtual servers (unordered).

show analytics http report view-by virtual measures {average-tps} limit 20 order-by { { measure average-tps sort-type desc } }

Gets the average tps of the top 20 virtual servers.

show analytics http report view-by virtual measures {average-tps} limit 20 order-by { { measure average-tps sort-type desc } } range now-3d--now

Gets the average tps of the top 20 virtual servers from the last three days.

show analytics http report view-by virtual drilldown { { entity application values { app } } { entity pool-member values { p1 p2 } } } range now-4d--now-2d measures {average-tps} limit 10 order-by { { measure average-tps sort-type DESC } }

Gets the average tps of the top 10 virtual servers (ordered by average tps) on **app** iApp (out of several monitored) on pool members **p1** and **p2**

show analytics http report view-by response-code drilldown { { entity virtual values { v1 } } } measures { transactions }

Gets a distribution of requests per response code on virtual v1.

show analytics http report view-by country drilldown { { entity application values { app } } } measures { average-concurrent-sessions average-sessions } order-by { { measure average-sessions sort-type DESC } } limit 5

Gets the new sessions and average concurrent sessions of the top five countries, ordered by the average concurrent sessions on the application **app**.

show analytics http report view-by client-ip drilldown { { entity virtual values { v1 } } } measures { max-page-load-time } limit 1

Gets the client IP address with the worst page load time.

show analytics http report view-by application drilldown { { entity pool-member values { p1 p2 } } } measures { transactions } order-by { { measure transactions } } range now-7d--now

Gets the distribution of requests per application on pool members *p1*

save analytics http report view-by virtual measures {average-tps} limit 20 order-by { { measure average-tps sort-type desc } } format pdf file report.pdf

Gets the average tps of the top 20 virtual servers and exports to a PDF file on the BIG-IP system.

save analytics http report view-by virtual measures {average-tps} limit 20 order-by { { measure average-tps sort-type desc } } format csv-aggregated file report.csv

Gets the average tps of the top 20 virtual servers and exports to a CSV file on the BIG-IP system.

save analytics http report view-by virtual measures {average-tps} limit 20 order-by { { measure average-tps sort-type desc } } format csv-time-series file report.csv

Gets the average tps over time of the top 10 virtual servers and exports to a CSV file on the BIG-IP system.

send-mail analytics http report view-by virtual measures {average-tps} limit 20 order-by { { measure average-tps sort-type desc } } format pdf email-addresses { some.one@someaddress.com }

Gets the average tps over time of the top 10 virtual servers and sends out an email containing the report as a PDF.

Options

- **device**
  Specifies a BIG-IP device on which to generate a report. (Enterprise Manager only)
- **device-list**
  Specifies a custom list of BIG-IP devices on which to generate a report. (Enterprise Manager only)
- **drilldown**
  Specifies specific entities that are used as a filter.
- **email-addresses**
  Specifies the list of email addresses to which the report file is sent when using the **send-mail** command.
- **file**
  Specifies the exported file path to be saved when using the **save** command. The file name should be simple (not a full path).
- **format**
  Specifies the exported file format to be saved or sent. This option must be specified when using the **save** or **send-mail** commands.
- **include-others**
  Specifies that the grand total for the measure is displayed for all entities, except for those shown in the result. It can be used along with **include-total**.
- **include-total**
  Specifies that a total summary row should be added to the analytics report. For average measures, the total value is also an average.
- **limit**
  Specifies the maximum number of rows/entities in the output result set/file. The default value is **10**, not including the total row/entity. The maximum value is **1000**.
- **measures**
  Specifies a list of measures that can be used with the chosen entity type. The default value is **transactions**. The options are:
  - **average-concurrent-sessions**
    The average number of concurrent sessions for each entity.
  - **average-new-sessions**
    The average number of new sessions for each entity.
  - **average-page-load-time**
    The average client page load time for each entity.
  - **average-request-throughput**
    The average request throughput for each entity.

- **average-response-throughput**
  The average response throughput for each entity.
- **average-server-latency**
  The average server latency for each entity.
- **average-tps**
  The average number of transactions per second for each entity.
- **client-side-sampled-transactions**
  The number of transactions sampled for client side page load time.
- **max-page-load-time**
  The maximum client page load time for each entity.
- **max-request-throughput**
  The maximum request throughput for each entity.
- **max-response-throughput**
  The maximum response throughput for each entity.
- **max-server-latency**
  The maximum server latency for each entity.
- **max-tps**
  The maximum number of transactions per second for each entity.
- **transactions**
  The absolute number of transactions for each entity.

◆ **order-by**
Specifies the measures and sort type (ascending or descending) that will be used to sort the final report. The default value for measures is previously chosen measures. The default value for sort type is **desc** (descending).

◆ **range**
Specifies the time/date range of the analytics information that you want to display. The given results will reflect the time range chosen here. The default value is the last hour (now--now-1h).

◆ **smtp-config-override**
Specifies the SMTP configuration to use when sending reports by email. This overrides the default SMTP settings.

See Also

show, *save*, *send-mail*, *tmsh*, *analytics*, *report*

16

analytics ip-layer

- Introducing the analytics ip-layer module
- Alphabetical list of components

Introducing the analytics ip-layer module

You can use the tmsh components that reside within the analytics IP-layer module to generate analytics reports. For more information about the tmsh hierarchical structure, see Chapter 2, *Understanding and Using the Traffic Management Shell*.

Alphabetical list of components

The remainder of this chapter lists the tmsh components that are available in the analytics IP-layer module.

report

Displays an ip-layer analytics report.

Syntax

Show, save or send an **analytics ip-layer report** using the syntax shown in the following sections.

Display

```
show report view-by [ ip ]
  drilldown {
    {
        entity [ ip ]
        values
        {
          [value ...]
        }
    } ...
  }
  field-fmt
  include-total
  include-others
  limit [number of rows]
  measures {
    [measure name ...]
  }
  order-by {
    {
      measure [ measure name ]
      sort-type [ asc / desc ]
    } ...
  }
  range [date range]
```

Save

```
save report view-by [ ip ]
   drilldown {
    {
        entity [ ip ]
        values
        {
          [value ...]
        }
    } ...
  }
  file [ file name ]
  format [ csv-aggregated | csv-time-series | pdf ]
  include-total
  include-others
  limit [number of rows]
  measures {
    [measure name ...]
  }
  order-by {
```

```
    {
      measure [ measure name ]
      sort-type [ asc / desc ]
    } ...
  }
  range [date range]
```

Send

```
send-mail report view-by [ ip ]
  drilldown {
    {
        entity [ ip ]
        values
        {
          [value ...]
        }
    } ...
  }
  email-addresses {
     [email address ...]
  }
  format [ csv-aggregated | csv-time-series | pdf ]
  include-total
  include-others
  limit [number of rows]
  measures {
    [measure name ...]
  }
  order-by {
    {
      measure [ measure name ]
      sort-type [ asc / desc ]
    } ...
  }
  range [date range]
  smtp-config-override [ smtp configuration object name ]
```

Description

Use this command to generate ip-layer analytics reports. You can generate a IP-layer analytics report for the following entities:

- **ip** - IP version (IPV4 / IPV6)

Different measures are collected for each of these entities and can be a part of the report request.

Examples

show analytics ip-layer report view-by ip

show analytics ip-layer report view-by ip drilldown { { entity ip values { IP-V4 } } }

send-mail analytics ip-layer report view-by ip measures { dropped-pkts } limit 20 order-by { { measure dropped-pkts sort-type desc } } format pdf email-addresses { some.one@someaddress.com }

For more syntactical examples, see the tmsh help manual for **analytics report**.

Options

- **device**
  Specifies a BIG-IP device on which to generate a report. (Enterprise Manager only)
- **device-list**
  Specifies a custom list of BIG-IP devices on which to generate a report. (Enterprise Manager only)
- **drilldown**
  Specifies specific entities that are used as a filter.
- **email-addresses**
  Specifies the list of email addresses to which the report file is sent when using the **send-mail** command.
- **file**
  Specifies the exported file path to be saved when using the **save** command. The file name should be simple (not a full path).
- **format**
  Specifies the exported file format to be saved or sent. This option must be specified when using the **save** or **send-mail** commands.
- **include-others**
  Specifies that the grand total for the measure is displayed for all entities, except for those shown in the result. It can be used along with **include-total**.
- **include-total**
  Specifies that a total summary row should be added to the analytics report. For average measures, the total value is also an average.
- **limit**
  Specifies the maximum number of rows/entities in the output result set/file. The default value is **10**, not including the total row/entity. The maximum value is **1000**.
- **measures**
  Specifies a list of measures that can be used with the chosen entity type. The options are:
  - **transmitted-pkts**
    The total number of ransmitted packets for the selected filter (entity).
  - **recieved-pkts**
    The total number of received packets for the selected filter (entity).
  - **dropped-pkts**
    The total number of dropped packets for the selected filter (entity).

- **err-invalid-len**
  The total number of error invalid length for the selected filter (entity).
- **err-memory**
  The total number of error memory for the selected filter (entity).
- **err-retransmitted**
  The total number of error retransmitted for the selected filter (entity).
- **err-protocol**
  The total number of error protocol for the selected filter (entity).
- **err-options**
  The total number of error options for the selected filter (entity).
- **err-checksum**
  The total number of error checksum for the selected filter (entity).
- **recieved-frags**
  The total number of received fragments for the selected filter (entity).
- **recieved_dropped_frags**
  The total number of received dropped fragments for the selected filter (entity).
- **transmitted-frags**
  The total number of transmitted fragments for the selected filter (entity).
- **transmitted-dropped-frags**
  The total number of transmitted dropped fragment for the selected filter (entity).
- **reassembled-frags**
  The total number of eassembled fragment for the selected filter (entity).
- **reassembled-dropped-frags**
  The total number of ‘too long’ reassembled dropped fragment for the selected filter (entity).

◆ **order-by**
Specifies the measures and sort type (ascending or descending) that will be used to sort the final report. The value for each measure is a previously chosen measure. The default value for sort type is **desc** (descending).

◆ **range**
Specifies the time/date range of the analytics information that you want to display. The given results will reflect the time range chosen here. The default value is the last hour (now--now-1h).

◆ **smtp-config-override**
Specifies the SMTP configuration to use when sending reports by email. This overrides the default SMTP settings.

See Also

show, *save*, *send-mail*, *tmsh*, *analytics*, *analytics*, *report*

17

analytics memory

- Introducing the analytics memory module
- Alphabetical list of components

Introducing the analytics memory module

You can use the tmsh components that reside within the analytics memory module to generate analytics reports. For more information about the tmsh hierarchical structure, see Chapter 2, *Understanding and Using the Traffic Management Shell*.

Alphabetical list of components

The remainder of this chapter lists the tmsh components that are available in the analytics memory module.

report

Displays an memory analytics report.

Syntax

Show, save or send an **analytics memory report** using the syntax shown in the following sections.

Display

```
show report view-by [ slot ]
  drilldown {
    {
        entity [ slot ]
        values
        {
          [value ...]
        }
    } ...
  }
  field-fmt
  include-total
  include-others
  limit [number of rows]
  measures {
    [measure name ...]
  }
  order-by {
    {
      measure [ measure name ]
      sort-type [ asc / desc ]
    } ...
  }
  range [date range]
```

Save

```
save report view-by [ slot ]
   drilldown {
    {
        entity [ slot ]
        values
        {
          [value ...]
        }
    } ...
  }
  file [ file name ]
  format [ csv-aggregated | csv-time-series | pdf ]
  include-total
  include-others
  limit [number of rows]
  measures {
    [measure name ...]
  }
  order-by {
```

```
    {
      measure [ measure name ]
      sort-type [ asc / desc ]
    } ...
  }
  range [date range]
```

Send

```
send-mail report view-by [ slot ]
  drilldown {
    {
        entity [ slot ]
        values
        {
          [value ...]
        }
    } ...
  }
  email-addresses {
     [email address ...]
  }
  format [ csv-aggregated | csv-time-series | pdf ]
  include-total
  include-others
  limit [number of rows]
  measures {
    [measure name ...]
  }
  order-by {
    {
      measure [ measure name ]
      sort-type [ asc / desc ]
    } ...
  }
  range [date range]
  smtp-config-override [ smtp configuration object name ]
```

Description

Use this command to generate memory analytics reports. You can generate a memory analytics report for the following entities:

- **slot** - Slot ID

Different measures are collected for each of these entities and can be a part of the report request.

Examples

show analytics memory report view-by slot

show analytics memory report view-by slot drilldown { { entity slot values { IP-V4 } } }

send-mail analytics memory report view-by slot measures { dropped-pkts } limit 20 order-by { { measure host-usage sort-type desc } } format pdf email-addresses { some.one@someaddress.com }

For more syntactical examples, see the tmsh help manual for **analytics report**.

Options

- **device**
  Specifies a BIG-IP device on which to generate a report. (Enterprise Manager only)
- **device-list**
  Specifies a custom list of BIG-IP devices on which to generate a report. (Enterprise Manager only)
- **drilldown**
  Specifies specific entities that are used as a filter.
- **email-addresses**
  Specifies the list of email addresses to which the report file is sent when using the **send-mail** command.
- **file**
  Specifies the exported file path to be saved when using the **save** command. The file name should be simple (not a full path).
- **format**
  Specifies the exported file format to be saved or sent. This option must be specified when using the **save** or **send-mail** commands.
- **include-others**
  Specifies that the grand total for the measure is displayed for all entities, except for those shown in the result. It can be used along with **include-total**.
- **include-total**
  Specifies that a total summary row should be added to the analytics report. For average measures, the total value is also an average.
- **limit**
  Specifies the maximum number of rows/entities in the output result set/file. The default value is **10**, not including the total row/entity. The maximum value is **1000**.
- **measures**
  Specifies a list of measures that can be used with the chosen entity type. The options are:
  - **tmm-total-ram**The avrerage of total TMM memory for the selected filter (entity).
  - **tmm-used-ram**The avrerage of used TMM memory for the selected filter (entity).

- **tmm-free-ram**The avrerage of free TMM memory for the selected filter (entity).
- **other-total-ram**The avrerage of total other (daemons and kernel) memory for the selected filter (entity).
- **other-used-ram**The avrerage of used other (daemons and kernel) memory for the selected filter (entity).
- **other-free-ram**The avrerage of free other (daemons and kernel) memory for the selected filter (entity).
- **system-total-ram**The avrerage of total system memory for the selected filter (entity).
- **system-used-ram**The avrerage of used system memory for the selected filter (entity).
- **system-free-ram**The avrerage of free system memory for the selected filter (entity).
- **swap-total-ram**The avrerage of total swap memory for the selected filter (entity).
- **swap-used-ram**The avrerage of used swap memory for the selected filter (entity).
- **swap-free-ram**The avrerage of free swap memory for the selected filter (entity).

◆ **order-by**
Specifies the measures and sort type (ascending or descending) that will be used to sort the final report. The value for each measure is a previously chosen measure. The default value for sort type is **desc** (descending).

◆ **range**
Specifies the time/date range of the analytics information that you want to display. The given results will reflect the time range chosen here. The default value is the last hour (now--now-1h).

◆ **smtp-config-override**
Specifies the SMTP configuration to use when sending reports by email. This overrides the default SMTP settings.

See Also

show, *save*, *send-mail*, *tmsh*, *analytics*, *analytics*, *report*

18

analytics network

- Introducing the analytics network module
- Alphabetical list of components

Introducing the analytics network module

You can use the tmsh components that reside within the analytics network module to generate analytics reports. For more information about the tmsh hierarchical structure, see Chapter 2, *Understanding and Using the Traffic Management Shell*.

Alphabetical list of components

The remainder of this chapter lists the tmsh components that are available in the analytics pem module.

report

Displays a network firewall analytics report.

Syntax

Show, save or send an **analytics network report** using the syntax shown in the following sections.

Display

```
show report view-by [ l3l4-errors-error-reason | l3l4-errors-network-protocol |
l3l4-errors-action | l3l4-errors-source-ip | l3l4-errors-destination-ip |
l3l4-errors-vlan |
                      acl-enforced-application | acl-enforced-destination-ip |
acl-enforced-destination-port | acl-enforced-policy | acl-enforced-rule |
                      acl-enforced-rule-action | acl-enforced-rule-context |
acl-enforced-rule-context-type | acl-enforced-self-ip | acl-enforced-server-ip |
                      acl-enforced-source-ip | acl-enforced-source-port |
acl-enforced-translation-pool | acl-enforced-translation-type | acl-enforced-vlan |
                      acl-mgmt-application | acl-mgmt-destination-ip |
acl-mgmt-destination-port | acl-mgmt-rule | acl-mgmt-rule-action |
                    acl-mgmt-rule-context | acl-mgmt-source-ip | acl-mgmt-source-port
|
                      acl-staged-application | acl-staged-destination-ip |
acl-staged-destination-port | acl-staged-policy | acl-staged-rule |
                      acl-staged-rule-action | acl-staged-rule-context |
acl-staged-rule-context-type | acl-staged-self-ip | acl-staged-server-ip |
                      acl-staged-source-ip | acl-staged-source-port |
acl-staged-translation-pool | acl-staged-translation-type | acl-staged-vlan ]
  drilldown {
    {
        entity [ l3l4-errors-error-reason | l3l4-errors-network-protocol |
l3l4-errors-action | l3l4-errors-source-ip | l3l4-errors-destination-ip |
l3l4-errors-vlan |
                  acl-enforced-application | acl-enforced-destination-ip |
acl-enforced-destination-port | acl-enforced-policy | acl-enforced-rule |
                  acl-enforced-rule-action | acl-enforced-rule-context |
acl-enforced-rule-context-type | acl-enforced-self-ip | acl-enforced-server-ip |
                  acl-enforced-source-ip | acl-enforced-source-port |
acl-enforced-translation-pool | acl-enforced-translation-type | acl-enforced-vlan |
                  acl-mgmt-application | acl-mgmt-destination-ip |
acl-mgmt-destination-port | acl-mgmt-rule | acl-mgmt-rule-action |
                  acl-mgmt-rule-context | acl-mgmt-source-ip | acl-mgmt-source-port  |
                  acl-staged-application | acl-staged-destination-ip |
acl-staged-destination-port | acl-staged-policy | acl-staged-rule |
                  acl-staged-rule-action | acl-staged-rule-context |
acl-staged-rule-context-type | acl-staged-self-ip | acl-staged-server-ip |
                  acl-staged-source-ip | acl-staged-source-port |
acl-staged-translation-pool | acl-staged-translation-type | acl-staged-vlan ]
        values
        {
          [value ...]
        }
    } ...
  }
  field-fmt
```

```
  include-total
  include-others
  limit [number of rows]
  measures {
    [measure name ...]
  }
  order-by {
    {
      measure [ measure name ]
      sort-type [ asc | desc ]
    } ...
  }
  range [date range]
```

Save

```
save report view-by [ l314-errors-error-reason | l314-errors-network-protocol |
l314-errors-action | l314-errors-source-ip | l314-errors-destination-ip |
l314-errors-vlan |
                      acl-enforced-application | acl-enforced-destination-ip |
acl-enforced-destination-port | acl-enforced-policy | acl-enforced-rule |
                      acl-enforced-rule-action | acl-enforced-rule-context |
acl-enforced-rule-context-type | acl-enforced-self-ip | acl-enforced-server-ip |
                      acl-enforced-source-ip | acl-enforced-source-port |
acl-enforced-translation-pool | acl-enforced-translation-type | acl-enforced-vlan |
                      acl-mgmt-application | acl-mgmt-destination-ip |
acl-mgmt-destination-port | acl-mgmt-rule | acl-mgmt-rule-action |
                    acl-mgmt-rule-context | acl-mgmt-source-ip | acl-mgmt-source-port
|
                      acl-staged-application | acl-staged-destination-ip |
acl-staged-destination-port | acl-staged-policy | acl-staged-rule |
                      acl-staged-rule-action | acl-staged-rule-context |
acl-staged-rule-context-type | acl-staged-self-ip | acl-staged-server-ip |
                      acl-staged-source-ip | acl-staged-source-port |
acl-staged-translation-pool | acl-staged-translation-type | acl-staged-vlan ]
   drilldown {
    {
        entity [ l314-errors-error-reason | l314-errors-network-protocol |
l314-errors-action | l314-errors-source-ip | l314-errors-destination-ip |
l314-errors-vlan |
                  acl-enforced-application | acl-enforced-destination-ip |
acl-enforced-destination-port | acl-enforced-policy | acl-enforced-rule |
                  acl-enforced-rule-action | acl-enforced-rule-context |
acl-enforced-rule-context-type | acl-enforced-self-ip | acl-enforced-server-ip |
                  acl-enforced-source-ip | acl-enforced-source-port |
acl-enforced-stranslation-pool | acl-enforced-translation-type | acl-enforced-vlan |
                  acl-mgmt-application | acl-mgmt-destination-ip |
acl-mgmt-destination-port | acl-mgmt-rule | acl-mgmt-rule-action |
                  acl-mgmt-rule-context | acl-mgmt-source-ip | acl-mgmt-source-port  |
                  acl-staged-application | acl-staged-destination-ip |
acl-staged-destination-port | acl-staged-policy | acl-staged-rule |
                  acl-staged-rule-action | acl-staged-rule-context |
acl-staged-rule-context-type | acl-staged-self-ip | acl-staged-server-ip |
                  acl-staged-source-ip | acl-staged-source-port |
acl-staged-translation-pool | acl-staged-translation-type | acl-staged-vlan ]
        values
        {
          [value ...]
        }
    } ...
  }
```

```
  file [ file name ]
  format [ csv-aggregated | csv-time-series | pdf ]
  include-total
  include-others
  limit [number of rows]
  measures {
    [measure name ...]
  }
  order-by {
    {
      measure [ measure name ]
      sort-type [ asc | desc ]
    } ...
  }
  range [date range]
```

Send

```
send-mail report view-by [ l314-errors-error-reason | l314-errors-network-protocol |
l314-errors-action | l314-errors-source-ip | l314-errors-destination-ip |
l314-errors-vlan |
                           acl-enforced-application | acl-enforced-destination-ip |
acl-enforced-destination-port | acl-enforced-policy | acl-enforced-rule |
                           acl-enforced-rule-action | acl-enforced-rule-context |
acl-enforced-rule-context-type | acl-enforced-self-ip | acl-enforced-server-ip |
                           acl-enforced-source-ip | acl-enforced-source-port |
acl-enforced-translation-pool | acl-enforced-translation-type | acl-enforced-vlan |
                           acl-mgmt-application | acl-mgmt-destination-ip |
acl-mgmt-destination-port | acl-mgmt-rule | acl-mgmt-rule-action |
                           acl-mgmt-rule-context | acl-mgmt-source-ip |
acl-mgmt-source-port  |
                           acl-staged-application | acl-staged-destination-ip |
acl-staged-destination-port | acl-staged-policy | acl-staged-rule |
                           acl-staged-rule-action | acl-staged-rule-context |
acl-staged-rule-context-type | acl-staged-self-ip | acl-staged-server-ip |
                           acl-staged-source-ip | acl-staged-source-port |
acl-staged-translation-pool | acl-staged-translation-type | acl-staged-vlan ]
  drilldown {
    {
        entity [ l314-errors-error-reason | l314-errors-network-protocol |
l314-errors-action | l314-errors-source-ip | l314-errors-destination-ip |
l314-errors-vlan |
                acl-enforced-application | acl-enforced-destination-ip |
acl-enforced-destination-port | acl-enforced-policy | acl-enforced-rule |
                acl-enforced-rule-action | acl-enforced-rule-context |
acl-enforced-rule-context-type | acl-enforced-self-ip | acl-enforced-server-ip |
                acl-enforced-source-ip | acl-enforced-source-port |
acl-enforced-translation-pool | acl-enforced-translation-type | acl-enforced-vlan |
                acl-mgmt-application | acl-mgmt-destination-ip |
acl-mgmt-destination-port | acl-mgmt-rule | acl-mgmt-rule-action |
                acl-mgmt-rule-context | acl-mgmt-source-ip | acl-mgmt-source-port  |
                acl-staged-application | acl-staged-destination-ip |
acl-staged-destination-port | acl-staged-policy | acl-staged-rule |
                acl-staged-rule-action | acl-staged-rule-context |
acl-staged-rule-context-type | acl-staged-self-ip | acl-staged-server-ip |
                acl-staged-source-ip | acl-staged-source-port |
acl-staged-translation-pool | acl-staged-translation-type | acl-staged-vlan ]
        values
        {
          [value ...]
        }
```

```
  } ...
}
email-addresses {
   [email address ...]
}
format [ csv-aggregated | csv-time-series | pdf ]
include-total
include-others
limit [number of rows]
measures {
  [measure name ...]
}
order-by {
  {
    measure [ measure name ]
    sort-type [ asc | desc ]
  } ...
}
range [date range]
smtp-config-override [ smtp configuration object name ]
```

Description

Use this command to generate network firewall analytics reports. You can generate a network firewall analytics report for the following entities:

- **action** - Action taken (allowed/dropped).
- **acl-enforced-application** - Application services (ACL - Enforced).
- **acl-enforced-destination-ip** - Destination IP Address (ACL - Enforced).
- **acl-enforced-destination-port** - Destination IP Port (ACL - Enforced).
- **acl-enforced-policy** - Policy (ACL - Enforced).
- **acl-enforced-rule-action** - Rule Action (ACL - Enforced).
- **acl-enforced-rule-context** - Rule Context (ACL - Enforced).
- **acl-enforced-rule-context-type** - Rule Context Type (ACL - Enforced).
- **acl-enforced-rule** - Rule (ACL - Enforced).
- **acl-enforced-self-ip** - Self IP Address (ACL - Enforced).
- **acl-enforced-server-ip** - Server IP Address (ACL - Enforced).
- **acl-enforced-source-ip** - Source IP Address (ACL - Enforced).

- **acl-enforced-source-port** - Source IP Port (ACL - Enforced).
- **acl-enforced-translation-pool** - Translation Pool (ACL - Enforced).
- **acl-enforced-translation-type** - Translation Type (ACL - Enforced).
- **acl-enforced-vlan** - VLAN (ACL - Enforced).
- **acl-mgmt-application** - Application services (ACL - Management).
- **acl-mgmt-destination-ip** - Destination IP Address (ACL - Management).
- **acl-mgmt-destination-port** - Destination IP Port (ACL - Management).
- **acl-mgmt-rule-action** - Rule Action (ACL - Management).
- **acl-mgmt-rule-context** - Rule Context (ACL - Management).
- **acl-mgmt-rule** - Rule (ACL - Management).
- **acl-mgmt-source-ip** - Source IP Address (ACL - Management).
- **acl-mgmt-source-port** - Source IP Port (ACL - Management).
- **acl-staged-application** - Application services (ACL - Staged).
- **acl-staged-destination-ip** - Destination IP Address (ACL - Staged).
- **acl-staged-destination-port** - Destination IP Port (ACL - Staged).
- **acl-staged-policy** - Policy (ACL - Staged).
- **acl-staged-rule-action** - Rule Action (ACL - Staged).
- **acl-staged-rule-context** - Rule Context (ACL - Staged).
- **acl-staged-rule-context-type** - Rule Context Type (ACL - Staged).
- **acl-staged-rule** - Rule (ACL - Staged).
- **acl-staged-self-ip** - Self IP Address (ACL - Staged).

- **acl-staged-server-ip** - Server IP Address (ACL - Staged).
- **acl-staged-source-ip** - Source IP Address (ACL - Staged).
- **acl-staged-source-port** - Source IP Port (ACL - Staged).
- **acl-staged-translation-pool** - Translation Reason (ACL - Staged).
- **acl-staged-translation-type** - Translation Type (ACL - Staged).
- **acl-staged-vlan** - VLAN (ACL - Staged).
- **l3l4-errors-action** - Network firewall errors action.
- **l3l4-errors-destination-ip** - Destination IP address (Network firewall errors).
- **l3l4-errors-error-reason** - Network firewall error reason.
- **l3l4-errors-network-protocol** - Destination port (Network protocol).
- **l3l4-errors-source-ip** - Source IP address (Network firewall errors).
- **l3l4-errors-vlan** - VLAN (Network firewall errors).

Examples

show analytics network report view-by acl-enforced-rule

show analytics network report view-by acl-staged-vlan drilldown { { entity acl-staged-destination-port values { 80 } } }

send-mail analytics network report view-by acl-mgmt-source-ip limit 20 format pdf email-addresses { some.one@someaddress.com }

For more syntactical examples see manual for **analytics report**.

Options

- **device**
  Specifies a BIG-IP device on which to generate a report. (Enterprise Manager only)
- **device-list**
  Specifies a custom list of BIG-IP devices on which to generate a report. (Enterprise Manager only)

- **drilldown**
  Specifies specific entities that are used as a filter.
- **email-addresses**
  Specifies the list of email addresses to which the report file is sent when using the **send-mail** command.
- **file**
  Specifies the exported file path to be saved when using the **save** command. The file name should be simple (not a full path).
- **format**
  Specifies the exported file format to be saved or sent. This option must be specified when using the **save** or **send-mail** commands.
- **include-others**
  Specifies that the grand total for the measure is displayed for all entities, except for those shown in the result. It can be used along with **include-total**.
- **include-total**
  Specifies that a total summary row should be added to the analytics report. For average measures, the total value is also an average.
- **limit**
  Specifies the maximum number of rows/entities in the output result set/file. The default value is **10**, not including the total row/entity. The maximum value is **1000**.
- **measures**
  Specifies a list of measures that can be used with the chosen entity type. The options are:
  - **acl-matches**
    The total number of ACL rule matches. Applicable only to view-by entities starting with "acl-".
  - **errors**
    The total number of firewall errors. Applicable only to view-by entities starting with "l3l3-errors-".
- **order-by**
  Specifies the measures and sort type (ascending or descending) that will be used to sort the final report. The value for each measure is a previously chosen measure. The default value for sort type is **desc** (descending).
- **range**
  Specifies the time/date range of the analytics information that you want to display. The given results will reflect the time range chosen here. The default value is the last hour (now--now-1h).
- **smtp-config-override**
  Specifies the SMTP configuration to use when sending reports by email. This overrides the default SMTP settings.

See Also

show, *save*, *send-mail*, *tmsh*, *analytics*, *report*

stale-rules

Displays a network firewall stale rules report.

Syntax

Show an **analytics network stale-rules** report using the syntax shown in the following sections.

Display

```
show stale-rules type [ enforced | staged ]
options:
drilldown {
  {
      entity [ context | policy | rule-name ]
      values
      {
        [value ...]
      }
  } ...
}
field-fmt
first-rule-number [ value ]
number-of-rules [ value ]
range [ date range ]
```

Description

Use this command to generate network firewall stale rules reports. A stale rule is one that has had not hits, or very few hits, over a specified time period. The report is displayed in order from the least-hit rules (including rules with no hits) to the most hit rules. You can generate a stale rules report for either enforced or staged rules.

Examples

show analytics network stale-rules type enforced

Shows a stale rules report for enforced rules (either inline or not).

show analytics network stale-rules type staged drilldown { { entity context values { /Common/virtual_server_1 } } }

Shows a stale rules report for staged rules in the context of the virtual server /Common/virtual_server_1

show analytics network stale-rules type enforced number-of-rules 100 range now-1w

Shows a stale rules report for enforced rules. 100 rules are shown in the report.
This report is shown for the last week (including the last day).

show analytics network stale-rules type enforced first-rule-number 10 number-of-rules 100 range now-1w

Shows a stale rules report for enforced rules. The first least hit 9 rules are skipped, and 100 rules are shown in the report.
This report is shown for the last week (including the last day).

show analytics network stale-rules type enforced first-rule-number 10 number-of-rules 100 range now-1d--now-1w

Shows a stale rules report for enforced rules. The first least hit 9 rules are skipped, and 100 rules are shown in the report.
This report is shown for the last week, excluding the last day.

Options

- **drilldown**
  Specifies specific entities that are used as a filter.
- **field-fmt**
  Shows statistics in field format for the specified items.
- **first-rule-number**
  Specifies the first rule number being displayed (rules are ordered by hit count in an ascending order).
- **number-of-rules**
  Specifies the maximum number of firewall rules being displayed in the output result set. The default value is **10**.
- **range**
  Specifies the time/date range of the analytics information that you want to display. The given results will reflect the time range chosen here. The default value is the last hour (**now--now-1h**).

See Also

analytics, *report*, *settings*, *show*, *tmsh*

19

analytics pem

- Introducing the analytics pem module
- Alphabetical list of components

Introducing the analytics pem module

You can use the tmsh components that reside within the analytics PEM module to generate analytics reports. For more information about the tmsh hierarchical structure, see Chapter 2, *Understanding and Using the Traffic Management Shell*.

Alphabetical list of components

The remainder of this chapter lists the tmsh components that are available in the analytics pem module.

report

Displays an pem analytics report.

Syntax

Show, save or send an **analytics pem report** using the syntax shown in the following sections.

Display

```
show report view-by [ application | category | url-category | policy | service |
action | tower | subscribers ]
  drilldown {
    {
        entity [ application | category | url-category | policy | service | action |
tower | subscribers ]
        values
        {
          [value ...]
        }
    } ...
  }
  field-fmt
  include-total
  include-others
  limit [number of rows]
  measures {
    [measure name ...]
  }
  order-by {
    {
      measure [ measure name ]
      sort-type [ asc / desc ]
    } ...
  }
  range [date range]
```

Save

```
save report view-by [ application | category | url-category | policy | service |
action | tower | subscribers ]
   drilldown {
    {
        entity [ application | category | url-category | policy | service | action |
tower | subscribers ]
        values
        {
          [value ...]
        }
    } ...
  }
  file [ file name ]
  format [ csv-aggregated | csv-time-series | pdf ]
  include-total
  include-others
  limit [number of rows]
```

```
  measures {
    [measure name ...]
  }
  order-by {
    {
      measure [ measure name ]
      sort-type [ asc / desc ]
    } ...
  }
  range [date range]
```

Send

```
send-mail report view-by [ application | category | url-category | policy | service |
action | tower | subscribers ]
  drilldown {
    {
        entity [ application | category | url-category | policy | service | action |
tower | subscribers ]
        values
        {
          [value ...]
        }
    } ...
  }
  email-addresses {
     [email address ...]
  }
  format [ csv-aggregated | csv-time-series | pdf ]
  include-total
  include-others
  limit [number of rows]
  measures {
    [measure name ...]
  }
  order-by {
    {
      measure [ measure name ]
      sort-type [ asc / desc ]
    } ...
  }
  range [date range]
  smtp-config-override [ smtp configuration object name ]
```

Description

Use this command to generate pem analytics reports. You can generate a PEM analytics report for the following entities:

- **application** - Classification application
- **category** - Classification category
- **url-category** - URL category

- **policy** - Classification application policy
- **service** - Forwarding service (endpoint)
- **action** - PEM action (Gate, Forward, ICAP, Modify HTTP header, etc...)
- **tower** - Tower the subscriber communicates from
- **subscribers** - Subscribers summary statistics

Different measures are collected for each of these entities and can be a part of the report request.

Examples

show analytics pem report view-by category

show analytics pem report view-by category drilldown { { entity policy values { Some_Policy_Name } } }

send-mail analytics pem report view-by tower measures { total_bytes_in } limit 20 order-by { { measure total_bytes_in sort-type desc } } format pdf email-addresses { some.one@someaddress.com }

For more syntactical examples, see the tmsh help manual for **analytics report**.

Options

- **device**
  Specifies a BIG-IP device on which to generate a report. (Enterprise Manager only)
- **device-list**
  Specifies a custom list of BIG-IP devices on which to generate a report. (Enterprise Manager only)
- **drilldown**
  Specifies specific entities that are used as a filter.
- **email-addresses**
  Specifies the list of email addresses to which the report file is sent when using the **send-mail** command.
- **file**
  Specifies the exported file path to be saved when using the **save** command. The file name should be simple (not a full path).
- **format**
  Specifies the exported file format to be saved or sent. This option must be specified when using the **save** or **send-mail** commands.

- **include-others**
  Specifies that the grand total for the measure is displayed for all entities, except for those shown in the result. It can be used along with **include-total**.
- **include-total**
  Specifies that a total summary row should be added to the analytics report. For average measures, the total value is also an average.
- **limit**
  Specifies the maximum number of rows/entities in the output result set/file. The default value is **10**, not including the total row/entity. The maximum value is **1000**.
- **measures**
  Specifies a list of measures that can be used with the chosen entity type. The options are:
  - **hitcount**
    The total number of classified flows for the selected filter (entity).
  - **total-bytes-in**
    The total number of bytes received for the selected filter (entity).
  - **total-bytes-out**
    The total number of bytes sent for the selected filter (entity).
  - **total-flows-opened**
    The total number of flows (classified and non-classified) for the selected filter (entity).
  - **total-flows-closed**
    The total number of closed flows for the selected filter (entity).
  - **total-subscribers-login**
    The total number of login events for the selected filter (entity).
  - **total-subscribers-logout**
    The total number of logout events for the selected filter (entity).
  - **avg-distinct-apps**
    The average number of distinct applications for the selected filter (entity).
  - **avg-distinct-categories**
    The average number of distinct categories for the selected filter (entity).
- **order-by**
  Specifies the measures and sort type (ascending or descending) that will be used to sort the final report. The value for each measure is a previously chosen measure. The default value for sort type is **desc** (descending).
- **range**
  Specifies the time/date range of the analytics information that you want to display. The given results will reflect the time range chosen here. The default value is the last hour (now--now-1h).

- **smtp-config-override**
  Specifies the SMTP configuration to use when sending reports by email. This overrides the default SMTP settings.

See Also

show, *save*, *send-mail*, *tmsh*, *analytics*, *analytics*, *report*

20

analytics protocol-security

- Introducing the analytics protocol-security module
- Alphabetical list of components

Introducing the analytics protocol-security module

You can use the tmsh components that reside within the analytics protocol-security module to generate analytics reports. For more information about the tmsh hierarchical structure, see Chapter 2, *Understanding and Using the Traffic Management Shell*.

Alphabetical list of components

The remainder of this chapter lists the tmsh components that are available in the analytics protocol-security module.

report

Displays a Protocol Security analytics report.

Syntax

Show, save, or send an **analytics protocol-security report** using the syntax shown in the following sections.

Display

```
show report view-by [ application | virtual-server | ip | violation| request-type |
protocol-type ]
  drilldown {
    {
        entity [ application | virtual-server | ip | violation| request-type |
protocol-type ]
        values
        {
          [value ...]
        }
    } ...
  }
  field-fmt
  include-total
  include-others
  limit [number of rows]
  measures {
    [measure name ...]
  }
  order-by {
    {
      measure [ measure name ]
      sort-type [ asc / desc ]
    } ...
  }
  range [date range]
```

Save

```
save report view-by [ application | virtual-server | ip | violation| request-type |
protocol-type ]
   drilldown {
    {
        entity [ application | virtual-server | ip | violation| request-type |
protocol-type ]
        values
        {
          [value ...]
        }
    } ...
  }
  file [ file name ]
  format [ csv-aggregated | csv-time-series | pdf ]
  include-total
  include-others
  limit [number of rows]
```

```
  measures {
    [measure name ...]
  }
  order-by {
    {
      measure [ measure name ]
      sort-type [ asc / desc ]
    } ...
  }
  range [date range]
```

Send

```
send-mail report view-by [ application | virtual-server | ip | violation| request-type
| protocol-type ]
  drilldown {
    {
        entity [ application | virtual-server | ip | violation| request-type |
protocol-type ]
        values
        {
          [value ...]
        }
    } ...
  }
  email-addresses {
     [email address ...]
  }
  format [ csv-aggregated | csv-time-series | pdf ]
  include-total
  include-others
  limit [number of rows]
  measures {
    [measure name ...]
  }
  order-by {
    {
      measure [ measure name ]
      sort-type [ asc / desc ]
    } ...
  }
  range [date range]
  smtp-config-override [ smtp configuration object name ]
```

Description

Use this command to generate protocol-security analytics reports. You can generate a protocol-security analytics report for the following entities:

- **application** - Application services.
- **virtual-server** - Virtual servers.
- **ip** - Source IP addresses.

- **violation** - Violation types.
- **protocol-type** - Protocol type (HTTP/FTP/SMTP)
- **request-type** - PRequest type (Legal or Alarmed/Blocked/Dropped)

Different measures are collected for each of these entities and can be a part of the report request.

Examples

show analytics protocol-security report view-by protocol-type

show analytics protocol-security report view-by request-type drilldown { { entity protocol-type values { HTTP } } }

send-mail analytics protocol-security report view-by protocol-type measures {transactions} limit 20 order-by { { measure transactions sort-type desc } } format pdf email-addresses { some.one@someaddress.com }

For more syntactical examples, see the manpage for **analytics report**.

Options

- **device**
  Specifies a BIG-IP device on which to generate a report. (Enterprise Manager only)
- **device-list**
  Specifies a custom list of BIG-IP devices on which to generate a report. (Enterprise Manager only)
- **drilldown**
  Specifies specific entities that are used as a filter.
- **email-addresses**
  Specifies the list of email addresses to which the report file is sent when using the **send-mail** command.
- **file**
  Specifies the exported file path to be saved when using the **save** command. The file name should be simple (not a full path).
- **format**
  Specifies the exported file format to be saved or sent. This option must be specified when using the **save** or **send-mail** commands.
- **include-others**
  Specifies that the grand total for the measure is displayed for all entities, except for those shown in the result. It can be used along with **include-total**.

- **include-total**
  Specifies that a total summary row should be added to the analytics report. For average measures, the total value is also an average.
- **limit**
  Specifies the maximum number of rows/entities in the output result set/file. The default value is **10**, not including the total row/entity. The maximum value is **1000**.
- **measures**
  Specifies a list of measures that can be used with the chosen entity type. The options are:
  - **requests**
    Request count.
  - **occurences**
    Number of occurences for the selected filter (relevant for violation entitiy only)
- **order-by**
  Specifies the measures and sort type (ascending or descending) that will be used to sort the final report. The value for each measure is a previously chosen measure. The default value for sort type is **desc** (descending).
- **range**
  Specifies the time/date range of the analytics information that you want to display. The given results will reflect the time range chosen here. The default value is the last hour (now--now-1h).
- **smtp-config-override**
  Specifies the SMTP configuration to use when sending reports by email. This overrides the default SMTP settings.

See Also

show, *save*, *send-mail*, *tmsh*, *analytics*, *analytics*, *report*

21

analytics sip-dos

- Introducing the analytics sip-dos module
- Alphabetical list of components

Introducing the analytics sip-dos module

You can use the tmsh components that reside within the analytics sip-dos module to generate analytics reports. For more information about the tmsh hierarchical structure, see Chapter 2, *Understanding and Using the Traffic Management Shell*.

Alphabetical list of components

The remainder of this chapter lists the tmsh components that are available in the analytics protocol-security module.

report

Displays a SIP DoS analytics report.

Syntax

Show, save or send an **analytics sip-dos report** using the syntax shown in the following sections.

Display

```
show report view-by [ application | attack-id | attack-type | callee | caller | method
| src-ip | virtual | vlan ]
  drilldown {
    {
        entity [ application | attack-id | attack-type | callee | caller | method |
src-ip | virtual | vlan ]
        values
        {
          [value ...]
        }
    } ...
  }
  field-fmt
  include-total
  include-others
  limit [number of rows]
  measures {
    [measure name ...]
  }
  order-by {
    {
      measure [ measure name ]
      sort-type [ asc | desc ]
    } ...
  }
  range [date range]
```

Save

```
save report view-by [ application | attack-id | attack-type | callee | caller | method
| src-ip | virtual | vlan ]
   drilldown {
    {
        entity [ application | attack-id | attack-type | callee | caller | method |
src-ip | virtual | vlan ]
        values
        {
          [value ...]
        }
    } ...
  }
  file [ file name ]
  format [ csv-aggregated | csv-time-series | pdf ]
  include-total
  include-others
  limit [number of rows]
```

```
  measures {
    [measure name ...]
  }
  order-by {
    {
      measure [ measure name ]
      sort-type [ asc | desc ]
    } ...
  }
  range [date range]
```

Send

```
send-mail report view-by [ application | attack-id | attack-type | callee | caller |
method | src-ip | virtual | vlan ]
  drilldown {
    {
        entity [ application | attack-id | attack-type | callee | caller | method |
src-ip | virtual | vlan ]
        values
        {
          [value ...]
        }
    } ...
  }
  email-addresses {
     [email address ...]
  }
  format [ csv-aggregated | csv-time-series | pdf ]
  include-total
  include-others
  limit [number of rows]
  measures {
    [measure name ...]
  }
  order-by {
    {
      measure [ measure name ]
      sort-type [ asc | desc ]
    } ...
  }
  range [date range]
  smtp-config-override [ smtp configuration object name ]
```

Description

Use this command to generate SIP DoS analytics reports. You can generate a SIP DoS prevention analytics report for the following entities:

- **application** - Application services (iApp).
- **attack-id** - DoS attack ID.
- **attack-type** - DoS attack type.

- **callee** - Callee.
- **caller** - Caller.
- **method** - Methos.
- **src-ip** - Source IP Address.
- **vlan** - VLAN.

Examples

show analytics sip-dos report view-by attack-id

show analytics sip-dos report view-by attack-type drilldown { { entity method values { ACK } } }

send-mail analytics sip-dos report view-by callee limit 20 format pdf email-addresses { some.one@someaddress.com }

For more syntactical examples see manual for **analytics report**.

Options

- **device**
  Specifies a BIG-IP device on which to generate a report. (Enterprise Manager only)
- **device-list**
  Specifies a custom list of BIG-IP devices on which to generate a report. (Enterprise Manager only)
- **drilldown**
  Specifies specific entities that are used as a filter.
- **email-addresses**
  Specifies the list of email addresses to which the report file is sent when using the **send-mail** command.
- **file**
  Specifies the exported file path to be saved when using the **save** command. The file name should be simple (not a full path).
- **format**
  Specifies the exported file format to be saved or sent. This option must be specified when using the **save** or **send-mail** commands.
- **include-others**
  Specifies that the grand total for the measure is displayed for all entities, except for those shown in the result. This option must be used with the **drilldown** option. You can also use it along with **include-others**.

- **include-total**
  Specifies that a total summary row should be added to the analytics report. For average measures, the total value is also an average.
- **limit**
  Specifies the maximum number of rows/entities in the output result set/file. The default value is **10**, not including the total row/entity. The maximum value is **1000**.
- **measures**
  Specifies a list of measures that can be used with the chosen entity type. The options are:
  - **allowed-requests**
    The total number of packets that were recieved by the virtual server(/s)s
  - **dropped-requests**
    The total number of packets that were dropped by the virtual server(/s)s
  - **total-requests**
    The total number of packets that were recieved or dropped by the virtual server(/s)s
- **order-by**
  Specifies the measures and sort type (ascending or descending) that will be used to sort the final report. The value for each measure is a previously chosen measure. The default value for sort type is **desc** (descending).
- **range**
  Specifies the time/date range of the analytics information that you want to display. The given results will reflect the time range chosen here. The default value is the last hour (now--now-1h).
- **smtp-config-override**
  Specifies the SMTP configuration to use when sending reports by email. This overrides the default SMTP settings.

See Also

show, *save*, *send-mail*, *tmsh*, *analytics*, *report*

22

analytics swg

- Introducing the analytics swg module
- Alphabetical list of components

Introducing the analytics swg module

You can use the tmsh components that reside within the analytics SWG module to generate analytics reports. For more information about the tmsh hierarchical structure, see Chapter 2, *Understanding and Using the Traffic Management Shell*.

Alphabetical list of components

The remainder of this chapter lists the tmsh components that are available in the analytics SWG module.

report

Displays an swg analytics report.

Syntax

Show, save or send an **analytics swg report** using the syntax shown in the following sections.

Display

```
show report view-by [ action | ssl_bypass | username | client_ip | url | category |
url_filter | filter_policy | host-name ]
  drilldown {
    {
        entity [ action | ssl_bypass | username | client_ip | url | category |
url_filter | filter_policy | host-name ]
        values
        {
          [value ...]
        }
    } ...
  }
  field-fmt
  include-total
  include-others
  limit [number of rows]
  measures {
    [measure name ...]
  }
  order-by {
    {
      measure [ measure name ]
      sort-type [ asc / desc ]
    } ...
  }
  range [date range]
```

Save

```
save report view-by [ action | ssl_bypass | username | client_ip | url | category |
url_filter | filter_policy | host-name ]
   drilldown {
    {
        entity [ action | ssl_bypass | username | client_ip | url | category |
url_filter | filter_policy | host-name ]
        values
        {
          [value ...]
        }
    } ...
  }
  file [ file name ]
  format [ csv-aggregated | csv-time-series | pdf ]
  include-total
  include-others
  limit [number of rows]
```

```
  measures {
    [measure name ...]
  }
  order-by {
    {
      measure [ measure name ]
      sort-type [ asc / desc ]
    } ...
  }
  range [date range]
```

Send

```
send-mail report view-by [ action | ssl_bypass | username | client_ip | url | category
| url_filter | filter_policy | host-name ]
  drilldown {
    {
        entity [ action | ssl_bypass | username | client_ip | url | category |
url_filter | filter_policy | host-name ]
        values
        {
          [value ...]
        }
    } ...
  }
  email-addresses {
     [email address ...]
  }
  format [ csv-aggregated | csv-time-series | pdf ]
  include-total
  include-others
  limit [number of rows]
  measures {
    [measure name ...]
  }
  order-by {
    {
      measure [ measure name ]
      sort-type [ asc / desc ]
    } ...
  }
  range [date range]
  smtp-config-override [ smtp configuration object name ]
```

Description

Use this command to generate swg analytics reports. You can generate an application-security-network analytics report for the following entities:

- **action** - Transction's action (Blocked / Allowed / Allowed with log)
- **ssl_bypass** - Is HTTP/HTPPS inspection bypassed
- **username** - User name

- **client-ip** - Client IP
- **host-name** - Host name
- **url** - URL
- **category** - URL category
- **url-filter** - URL filter
- **scheme** - Scheme

Different measures are collected for each of these entities and can be a part of the report request.

Examples

show analytics swg report view-by client-ip

show analytics swg report view-by client-ip drilldown { { entity scheme values { my_scheme } } }

send-mail analytics swg report view-by category measures { blocked-count } limit 20 order-by { { measure blocked-count sort-type desc } } format pdf email-addresses { some.one@someaddress.com }

For more syntactical examples, see the tmsh help manual for **analytics report**.

Options

- **device**
  Specifies a BIG-IP device on which to generate a report. (Enterprise Manager only)
- **device-list**
  Specifies a custom list of BIG-IP devices on which to generate a report. (Enterprise Manager only)
- **drilldown**
  Specifies specific entities that are used as a filter.
- **email-addresses**
  Specifies the list of email addresses to which the report file is sent when using the **send-mail** command.
- **file**
  Specifies the exported file path to be saved when using the **save** command. The file name should be simple (not a full path).

- **format**
  Specifies the exported file format to be saved or sent. This option must be specified when using the **save** or **send-mail** commands.
- **include-others**
  Specifies that the grand total for the measure is displayed for all entities, except for those shown in the result. It can be used along with **include-total**.
- **include-total**
  Specifies that a total summary row should be added to the analytics report. For average measures, the total value is also an average.
- **limit**
  Specifies the maximum number of rows/entities in the output result set/file. The default value is **10**, not including the total row/entity. The maximum value is **1000**.
- **measures**
  Specifies a list of measures that can be used with the chosen entity type. The options are:
  - **request-count**
    The total number of requests for the selected filter (entity).
- **order-by**
  Specifies the measures and sort type (ascending or descending) that will be used to sort the final report. The value for each measure is a previously chosen measure. The default value for sort type is **desc** (descending).
- **range**
  Specifies the time/date range of the analytics information that you want to display. The given results will reflect the time range chosen here. The default value is the last hour (now--now-1h).
- **smtp-config-override**
  Specifies the SMTP configuration to use when sending reports by email. This overrides the default SMTP settings.

See Also

show, *save*, *send-mail*, *tmsh*, *analytics*, *analytics*, *report*

23

analytics swg-blocked

- Introducing the analytics swg-blocked module
- Alphabetical list of components

Introducing the analytics swg-blocked module

You can use the tmsh components that reside within the analytics SWG-blocked module to generate analytics reports. For more information about the tmsh hierarchical structure, see Chapter 2, *Understanding and Using the Traffic Management Shell*.

Alphabetical list of components

The remainder of this chapter lists the tmsh components that are available in the analytics SWG-blocked module.

report

Displays an swg-blocked analytics report.

Syntax

Show, save or send an **analytics swg-blocked report** using the syntax shown in the following sections.

Display

```
show report view-by [ ssl_bypass | username | client_ip | url | category | url_filter |
filter_policy | security-category | host-name ]
  drilldown {
    {
        entity [ ssl_bypass | username | client_ip | url | category | url_filter |
filter_policy | security-category | host-name ]
        values
        {
          [value ...]
        }
    } ...
  }
  field-fmt
  include-total
  include-others
  limit [number of rows]
  measures {
    [measure name ...]
  }
  order-by {
    {
      measure [ measure name ]
      sort-type [ asc / desc ]
    } ...
  }
  range [date range]
```

Save

```
save report view-by [ ssl_bypass | username | client_ip | url | category | url_filter |
filter_policy | security-category | host-name ]
   drilldown {
    {
        entity [ ssl_bypass | username | client_ip | url | category | url_filter |
filter_policy | security-category | host-name ]
        values
        {
          [value ...]
        }
    } ...
  }
  file [ file name ]
  format [ csv-aggregated | csv-time-series | pdf ]
  include-total
  include-others
  limit [number of rows]
```

```
  measures {
    [measure name ...]
  }
  order-by {
    {
      measure [ measure name ]
      sort-type [ asc / desc ]
    } ...
  }
  range [date range]
```

Send

```
send-mail report view-by [ ssl_bypass | username | client_ip | url | category |
url_filter | filter_policy | security-category | host-name ]
  drilldown {
    {
        entity [ ssl_bypass | username | client_ip | url | category | url_filter |
filter_policy | security-category | host-name ]
        values
        {
          [value ...]
        }
    } ...
  }
  email-addresses {
     [email address ...]
  }
  format [ csv-aggregated | csv-time-series | pdf ]
  include-total
  include-others
  limit [number of rows]
  measures {
    [measure name ...]
  }
  order-by {
    {
      measure [ measure name ]
      sort-type [ asc / desc ]
    } ...
  }
  range [date range]
  smtp-config-override [ smtp configuration object name ]
```

Description

Use this command to generate swg-blocked analytics reports. You can generate an application-security-network analytics report for the following entities:

- **ssl_bypass** - Is HTTP/HTPPS inspection bypassed
- **username** - User name
- **client-ip** - Client IP

- **host-name** - Host name
- **url** - URL
- **category** - URL category
- **security-category** - Categories which their parent is ‘Security’ category
- **url-filter** - URL filter
- **scheme** - Scheme

Different measures are collected for each of these entities and can be a part of the report request.

Examples

show analytics swg-blocked report view-by client-ip

show analytics swg-blocked report view-by client-ip drilldown { { entity scheme values { my_scheme } } }

send-mail analytics swg-blocked report view-by category measures { blocked-count } limit 20 order-by { { measure blocked-count sort-type desc } } format pdf email-addresses { some.one@someaddress.com }

For more syntactical examples, see the tmsh help manual for **analytics report**.

Options

- **device**
  Specifies a BIG-IP device on which to generate a report. (Enterprise Manager only)
- **device-list**
  Specifies a custom list of BIG-IP devices on which to generate a report. (Enterprise Manager only)
- **drilldown**
  Specifies specific entities that are used as a filter.
- **email-addresses**
  Specifies the list of email addresses to which the report file is sent when using the **send-mail** command.
- **file**
  Specifies the exported file path to be saved when using the **save** command. The file name should be simple (not a full path).

- **format**
  Specifies the exported file format to be saved or sent. This option must be specified when using the **save** or **send-mail** commands.
- **include-others**
  Specifies that the grand total for the measure is displayed for all entities, except for those shown in the result. It can be used along with **include-total**.
- **include-total**
  Specifies that a total summary row should be added to the analytics report. For average measures, the total value is also an average.
- **limit**
  Specifies the maximum number of rows/entities in the output result set/file. The default value is **10**, not including the total row/entity. The maximum value is **1000**.
- **measures**
  Specifies a list of measures that can be used with the chosen entity type. The options are:
  - **blocked-count**
    The total number of blocked requests for the selected filter (entity).
- **order-by**
  Specifies the measures and sort type (ascending or descending) that will be used to sort the final report. The value for each measure is a previously chosen measure. The default value for sort type is **desc** (descending).
- **range**
  Specifies the time/date range of the analytics information that you want to display. The given results will reflect the time range chosen here. The default value is the last hour (now--now-1h).
- **smtp-config-override**
  Specifies the SMTP configuration to use when sending reports by email. This overrides the default SMTP settings.

See Also

show, *save*, *send-mail*, *tmsh*, *analytics*, *analytics*, *report*

24

analytics tcp

- Introducing the analytics tcp module
- Alphabetical list of components

Introducing the analytics tcp module

You can use the tmsh components that reside within the analytics TCP module to generate analytics reports. For more information about the tmsh hierarchical structure, see Chapter 2, *Understanding and Using the Traffic Management Shell*.

Alphabetical list of components

The remainder of this chapter lists the tmsh components that are available in the analytics TCP module.

report

Displays an tcp analytics report.

Syntax

Show, save or send an **analytics tcp report** using the syntax shown in the following sections.

Display

```
show report view-by [ virtual | tcp ]
  drilldown {
    {
        entity [ virtual | tcp ]
        values
        {
          [value ...]
        }
    } ...
  }
  field-fmt
  include-total
  include-others
  limit [number of rows]
  measures {
    [measure name ...]
  }
  order-by {
    {
      measure [ measure name ]
      sort-type [ asc / desc ]
    } ...
  }
  range [date range]
```

Save

```
save report view-by [ virtual | tcp ]
   drilldown {
    {
        entity [ virtual | tcp ]
        values
        {
          [value ...]
        }
    } ...
  }
  file [ file name ]
  format [ csv-aggregated | csv-time-series | pdf ]
  include-total
  include-others
  limit [number of rows]
  measures {
    [measure name ...]
  }
  order-by {
```

```
    {
      measure [ measure name ]
      sort-type [ asc / desc ]
    } ...
  }
  range [date range]
```

Send

```
send-mail report view-by [ virtual | tcp ]
  drilldown {
    {
        entity [ virtual | tcp ]
        values
        {
          [value ...]
        }
    } ...
  }
  email-addresses {
     [email address ...]
  }
  format [ csv-aggregated | csv-time-series | pdf ]
  include-total
  include-others
  limit [number of rows]
  measures {
    [measure name ...]
  }
  order-by {
    {
      measure [ measure name ]
      sort-type [ asc / desc ]
    } ...
  }
  range [date range]
  smtp-config-override [ smtp configuration object name ]
```

Description

Use this command to generate tcp analytics reports. You can generate a TCP analytics report for the following entities:

- **virtual** - Virtual Server
- **tcp** - TCP Profile

Different measures are collected for each of these entities and can be a part of the report request.

Examples

show analytics tcp report view-by virtual

show analytics tcp report view-by virtual drilldown { { entity virtual values { 172.12.34.56 } } }

send-mail analytics tcp report view-by tcp measures { max-active-conns } limit 20 order-by { { measure max-active-conns sort-type desc } } format pdf email-addresses { some.one@someaddress.com }

For more syntactical examples, see the tmsh help manual for **analytics report**.

Options

- **device**
  Specifies a BIG-IP device on which to generate a report. (Enterprise Manager only)
- **device-list**
  Specifies a custom list of BIG-IP devices on which to generate a report. (Enterprise Manager only)
- **drilldown**
  Specifies specific entities that are used as a filter.
- **email-addresses**
  Specifies the list of email addresses to which the report file is sent when using the **send-mail** command.
- **file**
  Specifies the exported file path to be saved when using the **save** command. The file name should be simple (not a full path).
- **format**
  Specifies the exported file format to be saved or sent. This option must be specified when using the **save** or **send-mail** commands.
- **include-others**
  Specifies that the grand total for the measure is displayed for all entities, except for those shown in the result. It can be used along with **include-total**.
- **include-total**
  Specifies that a total summary row should be added to the analytics report. For average measures, the total value is also an average.
- **limit**
  Specifies the maximum number of rows/entities in the output result set/file. The default value is **10**, not including the total row/entity. The maximum value is **1000**.
- **measures**
  Specifies a list of measures that can be used with the chosen entity type. The options are:
  - **avg-active-conns**
    The average number of actice connections for the selected filter (entity).
  - **max-active-conns**
    The max number of active connections for the selected filter (entity).

- **total-accepts**
  The total number of accepted connections for the selected filter (entity).
- **total-accept_fails**
  The total number of denied accept connections for the selected filter (entity).
- **total-new-conns**
  The total number of new connections for the selected filter (entity).
- **total-failed-conns**
  The total number of failed connections for the selected filter (entity).
- **total-expired-conns**
  The total number of expired connections for the selected filter (entity).
- **total-abandoned-connections**
  The total number of abandoned connections for the selected filter (entity).
- **total-rst-packets**
  The total number of RST connections for the selected filter (entity).
- **total-malformed-segments**
  The total number of malformed connections for the selected filter (entity).
- **total-oo-segs**
  The total number of out of ordered segments for the selected filter (entity).
- **total-rx-cookie**
  The total number of received SYN cookies for the selected filter (entity).
- **total-rxbadcookies**
  The total number of received bad SYN cookies for the selected filter (entity).
- **total-hw-cookies**
  The total number of received HW SYN cookies for the selected filter (entity).
- **total-syncacheover**
  The total number of SYN cache overflow for the selected filter (entity).
- **total-txrexmits**
  The total number of retransmitted segments for the selected filter (entity).
- **total-sndpack**
  The total number of sent packets for the selected filter (entity).

◆ **order-by**
Specifies the measures and sort type (ascending or descending) that will be used to sort the final report. The value for each measure is a previously chosen measure. The default value for sort type is **desc** (descending).

- **range**
  Specifies the time/date range of the analytics information that you want to display. The given results will reflect the time range chosen here. The default value is the last hour (now--now-1h).
- **smtp-config-override**
  Specifies the SMTP configuration to use when sending reports by email. This overrides the default SMTP settings.

See Also

show, *save*, *send-mail*, *tmsh*, *analytics*, *analytics*, *report*

25

analytics udp

- Introducing the analytics udp module
- Alphabetical list of components

Introducing the analytics udp module

You can use the tmsh components that reside within the analytics UDP module to generate analytics reports. For more information about the tmsh hierarchical structure, see Chapter 2, *Understanding and Using the Traffic Management Shell*.

Alphabetical list of components

The remainder of this chapter lists the tmsh components that are available in the analytics UDP module.

report

Displays an udp analytics report.

Syntax

Show, save or send an **analytics udp report** using the syntax shown in the following sections.

Display

```
show report view-by [ virtual | udp ]
  drilldown {
    {
        entity [ virtual | udp ]
        values
        {
          [value ...]
        }
    } ...
  }
  field-fmt
  include-total
  include-others
  limit [number of rows]
  measures {
    [measure name ...]
  }
  order-by {
    {
      measure [ measure name ]
      sort-type [ asc / desc ]
    } ...
  }
  range [date range]
```

Save

```
save report view-by [ virtual | udp ]
   drilldown {
    {
        entity [ virtual | udp ]
        values
        {
          [value ...]
        }
    } ...
  }
  file [ file name ]
  format [ csv-aggregated | csv-time-series | pdf ]
  include-total
  include-others
  limit [number of rows]
  measures {
    [measure name ...]
  }
  order-by {
```

```
    {
      measure [ measure name ]
      sort-type [ asc / desc ]
    } ...
  }
  range [date range]
```

Send

```
send-mail report view-by [ virtual | udp ]
  drilldown {
    {
        entity [ virtual | udp ]
        values
        {
          [value ...]
        }
    } ...
  }
  email-addresses {
     [email address ...]
  }
  format [ csv-aggregated | csv-time-series | pdf ]
  include-total
  include-others
  limit [number of rows]
  measures {
    [measure name ...]
  }
  order-by {
    {
      measure [ measure name ]
      sort-type [ asc / desc ]
    } ...
  }
  range [date range]
  smtp-config-override [ smtp configuration object name ]
```

Description

Use this command to generate udp analytics reports. You can generate a UDP analytics report for the following entities:

- **virtual** - Virtual Server
- **udp** - UDP Profile

Different measures are collected for each of these entities and can be a part of the report request.

Examples

show analytics udp report view-by virtual

show analytics udp report view-by virtual drilldown { { entity virtual values { 172.12.34.56 } } }

send-mail analytics udp report view-by udp measures { max-active-conns } limit 20 order-by { { measure max-active-conns sort-type desc } } format pdf email-addresses { some.one@someaddress.com }

For more syntactical examples, see the tmsh help manual for **analytics report**.

Options

- **device**
  Specifies a BIG-IP device on which to generate a report. (Enterprise Manager only)
- **device-list**
  Specifies a custom list of BIG-IP devices on which to generate a report. (Enterprise Manager only)
- **drilldown**
  Specifies specific entities that are used as a filter.
- **email-addresses**
  Specifies the list of email addresses to which the report file is sent when using the **send-mail** command.
- **file**
  Specifies the exported file path to be saved when using the **save** command. The file name should be simple (not a full path).
- **format**
  Specifies the exported file format to be saved or sent. This option must be specified when using the **save** or **send-mail** commands.
- **include-others**
  Specifies that the grand total for the measure is displayed for all entities, except for those shown in the result. It can be used along with **include-total**.
- **include-total**
  Specifies that a total summary row should be added to the analytics report. For average measures, the total value is also an average.
- **limit**
  Specifies the maximum number of rows/entities in the output result set/file. The default value is **10**, not including the total row/entity. The maximum value is **1000**.
- **measures**
  Specifies a list of measures that can be used with the chosen entity type. The options are:
  - **avg-active-conns**
    The average number of actice connections for the selected filter (entity).

- **max-active-conns**
  The max number of active connections for the selected filter (entity).
- **total-accepts**
  The total number of accepted connections for the selected filter (entity).
- **total-accept_fails**
  The total number of denied accept connections for the selected filter (entity).
- **total-new-conns**
  The total number of new connections for the selected filter (entity).
- **total-failed-conns**
  The total number of failed connections for the selected filter (entity).
- **total-expired-conns**
  The total number of expired connections for the selected filter (entity).
- **total-received-datagrams**
  The total number of received datagrams for the selected filter (entity).
- **total-malformed-datagrams**
  The total number of malformed datagrams for the selected filter (entity).
- **total-icmp-unreachable**
  The total number of ICMP unreachable for the selected filter (entity).
- **total-bad-sum-datagrams**
  The total number of bad checksum datagrams for the selected filter (entity).
- **total-no-sum-datagrams**
  The total number of 'no checksum' datagrams for the selected filter (entity).
- **total-transmitted-datagrams**
  The total number of transmitted datagrams for the selected filter (entity).

◆ **order-by**
Specifies the measures and sort type (ascending or descending) that will be used to sort the final report. The value for each measure is a previously chosen measure. The default value for sort type is **desc** (descending).

◆ **range**
Specifies the time/date range of the analytics information that you want to display. The given results will reflect the time range chosen here. The default value is the last hour (now--now-1h).

◆ **smtp-config-override**
Specifies the SMTP configuration to use when sending reports by email. This overrides the default SMTP settings.

See Also

show, *save*, *send-mail*, *tmsh*, *analytics*, *analytics*, *report*

26

analytics vcmp

- Introducing the analytics vcmp module
- Alphabetical list of components

Introducing the analytics vcmp module

You can use the tmsh components that reside within the analytics VCMP module to generate analytics reports. For more information about the tmsh hierarchical structure, see Chapter 2, *Understanding and Using the Traffic Management Shell*.

Alphabetical list of components

The remainder of this chapter lists the tmsh components that are available in the analytics VCMP module.

report

Displays an vcmp analytics report.

Syntax

Show, save or send an **analytics vcmp report** using the syntax shown in the following sections.

Display

```
show report view-by [ guest | slot | interface ]
  drilldown {
    {
        entity [ guest | slot | interface ]
        values
        {
          [value ...]
        }
    } ...
  }
  field-fmt
  include-total
  include-others
  limit [number of rows]
  measures {
    [measure name ...]
  }
  order-by {
    {
      measure [ measure name ]
      sort-type [ asc / desc ]
    } ...
  }
  range [date range]
```

Save

```
save report view-by [ guest | slot | interface ]
   drilldown {
    {
        entity [ guest | slot | interface ]
        values
        {
          [value ...]
        }
    } ...
  }
  file [ file name ]
  format [ csv-aggregated | csv-time-series | pdf ]
  include-total
  include-others
  limit [number of rows]
  measures {
    [measure name ...]
  }
  order-by {
```

```
    {
      measure [ measure name ]
      sort-type [ asc / desc ]
    } ...
  }
  range [date range]
```

Send

```
send-mail report view-by [ guest | slot | interface ]
  drilldown {
    {
        entity [ guest | slot | interface ]
        values
        {
          [value ...]
        }
    } ...
  }
  email-addresses {
     [email address ...]
  }
  format [ csv-aggregated | csv-time-series | pdf ]
  include-total
  include-others
  limit [number of rows]
  measures {
    [measure name ...]
  }
  order-by {
    {
      measure [ measure name ]
      sort-type [ asc / desc ]
    } ...
  }
  range [date range]
  smtp-config-override [ smtp configuration object name ]
```

Description

Use this command to generate vcmp analytics reports. You can generate a vCMP analytics report for the following entities:

- **slot** - Slot ID
- **guest** - vCMP Guest name
- **interface** - vCMP Interface

Different measures are collected for each of these entities and can be a part of the report request.

Examples

show analytics vcmp report view-by slot

show analytics vcmp report view-by slot drilldown { { entity slot values { 5 } } }

send-mail analytics vcmp report view-by guest measures { network-bytes-in } limit 20 order-by { { measure network-bytes-in sort-type desc } } format pdf email-addresses { some.one@someaddress.com }

For more syntactical examples, see the tmsh help manual for **analytics report**.

Options

- **device**
  Specifies a BIG-IP device on which to generate a report. (Enterprise Manager only)
- **device-list**
  Specifies a custom list of BIG-IP devices on which to generate a report. (Enterprise Manager only)
- **drilldown**
  Specifies specific entities that are used as a filter.
- **email-addresses**
  Specifies the list of email addresses to which the report file is sent when using the **send-mail** command.
- **file**
  Specifies the exported file path to be saved when using the **save** command. The file name should be simple (not a full path).
- **format**
  Specifies the exported file format to be saved or sent. This option must be specified when using the **save** or **send-mail** commands.
- **include-others**
  Specifies that the grand total for the measure is displayed for all entities, except for those shown in the result. It can be used along with **include-total**.
- **include-total**
  Specifies that a total summary row should be added to the analytics report. For average measures, the total value is also an average.
- **limit**
  Specifies the maximum number of rows/entities in the output result set/file. The default value is **10**, not including the total row/entity. The maximum value is **1000**.
- **measures**
  Specifies a list of measures that can be used with the chosen entity type. The options are:

- **network-bytes-in**
  The total number of bytes received for the selected filter (entity).
- **network-bytes-out**
  The total number of bytes sent for the selected filter (entity).
- **network-average-in-throughput**
  The average received throughput for the selected filter (entity).
- **network-average-out-throughput**
  The average throughput sent for the selected filter (entity).
- **average-cpu-usage**
  The average number of CPU usage for the selected filter (entity).
- **diskio-bytes-read**
  The average number of bytes read from disk for the selected filter (entity).
- **diskio-bytes-written**
  The average number of bytes written to disk for the selected filter (entity).
- **diskio-requests-read**
  The average number of read requests from disk for the selected filter (entity).
- **diskio-requests-written**
  The average number of write requests from disk for the selected filter (entity).

◆ **order-by**
Specifies the measures and sort type (ascending or descending) that will be used to sort the final report. The value for each measure is a previously chosen measure. The default value for sort type is **desc** (descending).

◆ **range**
Specifies the time/date range of the analytics information that you want to display. The given results will reflect the time range chosen here. The default value is the last hour (now--now-1h).

◆ **smtp-config-override**
Specifies the SMTP configuration to use when sending reports by email. This overrides the default SMTP settings.

See Also

show, *save*, *send-mail*, *tmsh*, *analytics*, *analytics*, *report*

27

analytics virtual

- Introducing the analytics virtual module
- Alphabetical list of components

Introducing the analytics virtual module

You can use the tmsh components that reside within the analytics virtual module to generate analytics reports. For more information about the tmsh hierarchical structure, see Chapter 2, *Understanding and Using the Traffic Management Shell*.

Alphabetical list of components

The remainder of this chapter lists the tmsh components that are available in the analytics virtual module.

report

Displays an virtual analytics report.

Syntax

Show, save or send an **analytics virtual report** using the syntax shown in the following sections.

Display

```
show report view-by [ virtual ]
  drilldown {
    {
        entity [ virtual ]
        values
        {
          [value ...]
        }
    } ...
  }
  field-fmt
  include-total
  include-others
  limit [number of rows]
  measures {
    [measure name ...]
  }
  order-by {
    {
      measure [ measure name ]
      sort-type [ asc / desc ]
    } ...
  }
  range [date range]
```

Save

```
save report view-by [ virtual ]
   drilldown {
    {
        entity [ virtual ]
        values
        {
          [value ...]
        }
    } ...
  }
  file [ file name ]
  format [ csv-aggregated | csv-time-series | pdf ]
  include-total
  include-others
  limit [number of rows]
  measures {
    [measure name ...]
  }
  order-by {
```

```
    {
      measure [ measure name ]
      sort-type [ asc / desc ]
    } ...
  }
  range [date range]
```

Send

```
send-mail report view-by [ virtual ]
  drilldown {
    {
        entity [ virtual ]
        values
        {
          [value ...]
        }
    } ...
  }
  email-addresses {
     [email address ...]
  }
  format [ csv-aggregated | csv-time-series | pdf ]
  include-total
  include-others
  limit [number of rows]
  measures {
    [measure name ...]
  }
  order-by {
    {
      measure [ measure name ]
      sort-type [ asc / desc ]
    } ...
  }
  range [date range]
  smtp-config-override [ smtp configuration object name ]
```

Description

Use this command to generate virtual analytics reports. You can generate a VIP analytics report for the following entities:

- **virtual** - Virtual Server

Different measures are collected for each of these entities and can be a part of the report request.

Examples

show analytics virtual report view-by virtual

show analytics virtual report view-by virtual drilldown { { entity virtual values { 172.12.34.67 } } }

send-mail analytics virtual report view-by virtual measures { total-server-packets-in } limit 20 order-by { { measure total-server-packets-in sort-type desc } } format pdf email-addresses { some.one@someaddress.com }

For more syntactical examples, see the tmsh help manual for **analytics report**.

Options

- **device**
  Specifies a BIG-IP device on which to generate a report. (Enterprise Manager only)
- **device-list**
  Specifies a custom list of BIG-IP devices on which to generate a report. (Enterprise Manager only)
- **drilldown**
  Specifies specific entities that are used as a filter.
- **email-addresses**
  Specifies the list of email addresses to which the report file is sent when using the **send-mail** command.
- **file**
  Specifies the exported file path to be saved when using the **save** command. The file name should be simple (not a full path).
- **format**
  Specifies the exported file format to be saved or sent. This option must be specified when using the **save** or **send-mail** commands.
- **include-others**
  Specifies that the grand total for the measure is displayed for all entities, except for those shown in the result. It can be used along with **include-total**.
- **include-total**
  Specifies that a total summary row should be added to the analytics report. For average measures, the total value is also an average.
- **limit**
  Specifies the maximum number of rows/entities in the output result set/file. The default value is **10**, not including the total row/entity. The maximum value is **1000**.
- **measures**
  Specifies a list of measures that can be used with the chosen entity type. The options are:
  - **total-client-packets-in**
    The total number of client-side received packets for the selected filter (entity).
  - **total-client-packets-out**
    The total number of client-side sent packets for the selected filter (entity).

- **total-server-packets-in**
  The total number of server-side received packets for the selected filter (entity).
- **total-server-packets-out**
  The total number of server-side sent packets for the selected filter (entity).
- **total-client-bits-in**
  The total number of client-side received bits for the selected filter (entity).
- **total-client-bits-out**
  The total number of client-side sent bits for the selected filter (entity).
- **total-server-bits-in**
  The total number of server-side received bits for the selected filter (entity).
- **total-server-bits-out**
  The total number of server-side sent bits for the selected filter (entity).
- **total-client-conns**
  The total number of client-side connections for the selected filter (entity).
- **avg-client-concurrent-conns**
  The average number of client-side concurrent connections for the selected filter (entity).
- **max-client-concurrent-conns**
  The max value of client-side concurrent connections for the selected filter (entity).
- **total-server-conns**
  The total number of server-side connections for the selected filter (entity).
- **avg-server-concurrent-conns**
  The average number of server-side concurrent connections for the selected filter (entity).
- **max-server-concurrent-conns**
  The max value of server side concurrent connections for the selected filter (entity).
- **total-syncookies**
  The total number of syncookies for the selected filter (entity).
- **total-syncookies-accepts**
  The total number of accepted syncookies for the selected filter (entity).
- **total-syncookies-rejects**
  The total number of rejected syncookies for the selected filter (entity).
- **total-hw-syncookies**
  The total number of HW syncookies for the selected filter (entity).
- **total-hw-syncookies-accepts**
  The total number of accepted HW syncookies for the selected filter (entity).

- **order-by**
  Specifies the measures and sort type (ascending or descending) that will be used to sort the final report. The value for each measure is a previously chosen measure. The default value for sort type is **desc** (descending).
- **range**
  Specifies the time/date range of the analytics information that you want to display. The given results will reflect the time range chosen here. The default value is the last hour (now--now-1h).
- **smtp-config-override**
  Specifies the SMTP configuration to use when sending reports by email. This overrides the default SMTP settings.

See Also

show, *save*, *send-mail*, *tmsh*, *analytics*, *analytics*, *report*

28

apm

- Introducing the apm module
- Alphabetical list of components

Introducing the apm module

You can use the tmsh components that reside within the apm module to configure BIG-IP® Access Policy Manager®. For more information about the tmsh hierarchical structure, see Chapter 2, *Understanding and Using the Traffic Management Shell*.

Alphabetical list of components

The remainder of this chapter lists the tmsh components that are available in the apm module.

acl

Manages an access control list (ACL).

Syntax

Configure the **acl** component within the **apm** module using the syntax shown in the following sections.

Create/Modify

```
create acl [name]
modify acl [name]
    acl-order [integer]
    app-service [[string] | none]
    description [[string] | none]
    entries {
      {
          action [allow | continue | discard | reject | unspec]
   dst-end-port [[service] | none]
   dst-start-port [[service] | none]
   dst-subnet [[ip addr] | [[ip addr] [mask]]
   host [[string] | none]
   log [config | none | packet | summary | verbose]
   paths [[string] | none]
   protocol [integer]
   scheme [any | http | https}
   src-end-port [[service] | none]
   src-start-port [[service] | none]
   src-subnet [[ip addr] | [[ip addr] [mask]]
      }
    }
    location-specific [true | false]
    path-match-case [false | true]
    type [dynamic | static]
```

Display

```
list acl
list acl [ [ [name] | [glob] | [regex] ] ... ]
show running-config acl
show running-config acl [ [ [name] | [glob] | [regex] ] ... ]
     all-properties
     non-default-properties
     partition
show acl
show acl [name]
```

Delete

```
delete acl [name]
```

Description

You can use the **acl** component to configure a set of restrictions associated with a resource or favorite that defines access for users and groups.

Examples

- **create acl MyACL { acl-order 3 entries src-start-port ip default inet dst-end-port ip default inet action allow }**
  Creates the static access control list named **MyACL** that is the third ACL in the list of ACLs in the visual policy editor, and adds an access control entry that allows traffic using the default source IP address and the default destination IP address.
- **list acl all-properties**
  Displays a list of ACLs that includes the attributes of each ACL.
- **delete acl MyACL**
  Deletes the **MyACL** access control list.

Options

- **acl-order**
  Specifies the order of the access control entries in this access control list. This option is required.
- **app-service**
  Specifies the name of the application service to which the object belongs. The default value is **none**. **Note:** If the **strict-updates** option is **enabled** on the application service that owns the object, you cannot modify or delete the object. Only the application service can modify or delete the object.
- **description**
  Describes the access control list.
- **entries**
  Configures an entry for an access control list.
  - **action**
    Specifies the action that an access control list takes when this access control list entry is encountered. This option is required. You can specify one of the following actions:
    - **allow**
      Allows traffic.
    - **continue**
      Skips checking against the remaining access control list entries in this access control list, and continues evaluation at the next access control list.
    - **discard**
      Drops packets silently.

    - **reject**
      Drops a packet and sends TCP RST on TCP flows or proper ICMP messages on UDP flows. Silently drops a packet on other protocols.
- **dst-end-port**
  Specifies the destination IP address and network mask of the access control list entry. The default is **0**.
- **dst-start-port**
  Specifies the source port or range of ports of the access control list entry.
- **dst-subnet**
  Specifies the destination subnet.
- **host**
  Specifies the host name of the access control list entry.
- **location-specific**
  Specifies whether or not this object contains one or more attributes with values that are specific to the location where the BIG-IP device resides. The location-specific attribute is either true or false. When using policy sync, mark an object as location-specific to prevent errors that can occur when policies reference objects, such as authentication servers, that are specific to a certain location.
- **log**
  Specifies the log level that is logged when actions of this type occur. Your options are:
    - **config**
      Logs the configuration of a matched entry.
    - **none**
      Logs nothing. This is the default value.
    - **packet**
      Logs a matched packet.
    - **summary**
      Logs the name and entry number of a matched access control list and access control list entry.
    - **verbose**
      Logs everything.
- **paths**
  Specifies an L7 access control list of matching URL paths.
- **protocol**
  Specifies the protocol number (TCP=6, UDP=17) of the access control list entry. The default is **0**.
- **src-end-port**
  Specifies the source IP address and network mask of the access control list entry.
- **src-start-port**
  Specifies the source port or range of ports of the access control list entry.

- **src-subnet**
  Specifies the source subnet.

- **[name]**
  Specifies the name of the access control list. This setting is required.
- **partition**
  Displays the partition within which the object resides. The default is **Common**.
- **path-match-case**
  Indicates whether the path is case sensitive. The default is **true**.
- **type**
  Specifies the type of access control list. The default is **static**. The available types are **static** and **dynamic**.

apm-avr-config

Configures AVR overview/statistics settings for Secure Web Gateway Functionality

Syntax

Configure an **apm-avr-config** component within the **apm** module using the syntax shown in the following sections.

Modify

The AVR Configuration consists of the following information: boolean flag to turn off data collection by AVR; Boolean flag to turn off sampling by AVR; Both are on by default. No create or delete function is allowed.

```
modify apm-avr-config apm-avr-config {
    avr-collect-data [true | false]
    avr-sampling [true | false]
    }
```

Display

```
list apm-avr-config
list apm-avr-config [ [ [name] | [glob] | [regex] ] ... ]
    all-properties
    non-default-properties
    one-line
    partition
```

Description

Configures AVR Configuration for SWG Statistical Reporting

Examples

modify apm-avr-config apm-avr-config { avr-collect-data false }

Modify apm-avr-config by setting avr collect data to false.

Options

- **avr-collect-data**
  Specifies whether data should be collected or not for statistical reporting.
- **avr-sampling**
  Specifies whether sampling should be turned on or off.

log-setting

Configures log configurations for various features in APM, such as URL Filter/Classification (URL Filter).

Syntax

Configure the **log-setting** component within the <apm> module using the syntax shown in the following sections.

Create/Modify

Consider log-setting as a container for log configurations belonging to different features. At this time URL Filter is the only feature with a log setting.

```
create log-setting [name]
modify log-setting [name]
    description
    url-filters [add | delete | modify | replace-all-with] {
      [item name] {
        filter { log-allowed-url [true|false] log-blocked-url [true|false] }
        publisher [string]
      }
    }
```

Display

```
list log-setting
list log-setting [ [ [name] | [glob] | [regex] ] ... ]
    all-properties
    non-default-properties
    one-line
    partition
```

Description

Configures a container for log configurations.

NOTE: Each container can enclose log configurations for many different features. However, each feature can only have one log configuration in a container.

NOTE: For the log configuration to take effect, the log-setting must be associated with an access profile (See man page for apm access profile).

NOTE: A log-setting container cannot be deleted if it is associated with an access profile.

Examples

create log-setting my-log-cfg

Creates a container without any log configuration.

create log-setting my-log-cfg url-filters add { my-urlf { filter { log-allowed-url true } publisher my-publisher } }

Creates a container with a log configuration for the URL Filter feature. At this version, URL Filter is the only feature with a log configuration.

modify log-setting my-log-cfg url-filters modify { my-urlf { publisher my-other-publisher } }

Modify the publisher of a log configuration.

modify log-setting my-log-cfg url-filters modify { my-urlf { filter { log-allowed-url false } } }

Modify the setting of a log filter

Options

- **description**
  Specifies a unique description for the log-setting container.
- **url-filters**
  This is the list to store log configurations for the URL Filter feature.
- **item name**
  Specifies the name of the log configuration to be added to the list url-filters. Currently, the list supports only one item.
- **filter**
  Specifies the value for different log filters. In particular, URL Filter log configuration has two filters: log-allowed-url [true|false] log-blocked-url [true|false]
- **publisher**
  Specifies the publisher of the log configuration. See **sys log-config publisher**.

See Also

access and *sys log-config*

swg-scheme

Configures SWG Scheme and schedules

Syntax

Configure a **swg-scheme** component within the **apm** module using the syntax shown in the following sections.

Create/Modify

Each swg-scheme consists of the following: content-scanning options (none or recommended, buffer size, buffer time), and default SWG service failure action.

```
create swg-scheme [name]
    content-scanning [none | recommended]
    content-scanning-max-buffer-size [size in bytes]
    content-scanning-max-buffer-time [time in seconds]
    safe-search [enable | disable ]
    swg-service-failure-action [allow | block]
modify swg-scheme  [name]
    content-scanning [none | recommended]
    content-scanning-max-buffer-size [size in bytes]
    content-scanning-max-buffer-time [time in seconds]
    safe-search [enable | disable ]
    swg-service-failure-action [allow | block]
```

Display

```
list swg-scheme
list swg-scheme [ [ [name] | [glob] | [regex] ] ... ]
    all-properties
    non-default-properties
    one-line
    partition
```

Cp

```
cp swg-scheme [source-name] [target-name]
```

Description

Configures an swg-scheme object

Examples

create apm swg-scheme scheme1 { swg-service-failure-action block content-scanning none }

Creates a new swg-scheme.

modify swg-scheme scheme1 { content-scanning recommended}

Modify a swg-scheme by modifying content scanning option to recommended.

cp swg-scheme existing-scheme new-scheme

Create a new swg-scheme by copying from an existing scheme.

Options

- **content-scanning**
  Specifies the content scanning option. Valid values are recommended or none.
- **description**
  Specifies a unique description for the swg scheme.
- **safe-search**
  Enables or disables Safe Search filtering for supported search engines.
- **swg-service-failure-action**
  Specifies the default action in case of swg service failure. Valid values are allow or block.

See Also

url-filter

url-filter

Configures URL filters for URL classification and filtering

Syntax

Configure a **url-filter** component within the **apm** module using the syntax shown in the following sections.

Create/Modify

Each url-filter consists of two url-category lists: a list of allowed URL categories and a list of blocked URL categories. The requests for URLs contained in the allowed list are allowed to pass unfettered, whereas requests for URLs in the blocked list will not go out into the Internet.

```
create url-filter [name]
    allowed-categories [add | delete | modify | replace-all-with] {
        [string]
    }
    blocked-categories [add | delete | modify | replace-all-with] {
        [string]
    }
modify url-filter [name]
    allowed-categories [add | delete | modify | replace-all-with] {
        [string]
    }
    blocked-categories [add | delete | modify | replace-all-with] {
        [string]
    }
```

Display

```
list url-filter
list url-filter [ [ [name] | [glob] | [regex] ] ... ]
    all-properties
    non-default-properties
    one-line
    partition
```

Cp

```
cp url-filter [source-name] [target-name]
```

Description

Configures a url-filter

NOTE: A url-filter can have a large number of URL categories in each list. To facilitate the creation of url-filter, you can create a new url-filter by copying from an existing url-filter. Then modify each list by adding or removing url-categories to suit your needs.

Examples

create url-filter my-url-filter allowed-categories add { Business_and_Economy Education } blocked-categories add { Adult_Content Shopping }

Creates a new url-filter.

modify url-filter my-own-filter allowed-categories delete { Education }

Modify a url-filter by deleting a URL category from the allowed list.

cp url-filter existing-filter another-filter

Create a new url-filter by copying from an existing filter.

Options

- **allowed-categories**
  Specifies the URL categories that should be allowed to pass.
- **description**
  Specifies a unique description for the URL filter.
- **blocked-categories**
  Specifies the URL categories that should be blocked.

See Also

download-result download-schedule and sy url-db url-category

29

apm aaa

- Introducing the apm aaa module
- Alphabetical list of components

Introducing the apm aaa module

You can use the tmsh components that reside within the apm aaa module to configure BIG-IP® Access Policy Manager®. For more information about the tmsh hierarchical structure, see Chapter 2, *Understanding and Using the Traffic Management Shell*.

Alphabetical list of components

The remainder of this chapter lists the tmsh components that are available in the apm aaa module.

active-directory

Manages an authentication access policy (AAA) Active Directory® server.

Syntax

Configure the **active-directory** component within the **aaa** module using the syntax shown in the following sections.

Create/Modify

```
create active-directory [name]
modify active-directory [name]
    admin-encrypted-password [[string] | none]
    admin-name [[string] | none]
    app-service [[string] | none]
    cleanup-cache [pso | group | none]
    description [[string] | none]
    domain [[string] | none]
    domain-controller [[string] | none]
    domain-controllers [add | delete | modify | replace-all-with] {
       [name] {
         ip [ip address]
       }
    }
    group-cache-ttl [integer]
    domain-controllers none
    location-specific [true | false]
    pool [name]
    pso-cache-ttl [integer]
    padata [encryption type]
    timeout [[integer] | immediate | indefinite]
edit active-directory [ [ [name] | [glob] | [regex] ] ... ]
    all-properties
    non-default-properties
```

Display

```
list active-directory
list active-directory [ [ [name] | [glob] | [regex] ] ... ]
show running-config active-directory
show running-config active-directory [ [ [name] | [glob] | [regex] ] ... ]
    all-properties
    app-service
    non-default-properties
    one-line
    partition
show active-directory
show active-directory [name]
```

Delete

```
delete active-directory [name]
```

Description

You can use the **active-directory** component to manage an AAA Active Directory server. The Active Directory is a network structure supported by Windows® 2000, or later, that provides support for tracking and locating any object on a network.

Examples

- **create active-directory MyADserver {**
  domain-controller "server01.company.com
  domain "company.com
  "
  admin-name "administrator"
  admin-encrypted-password "!My123Password"
  }
  Creates the AAA Active Directory server named **MyADserver** in the **company.dom** domain, sets the administrator logon name to **administrator** and the administrator password to **!My123Password**, and sets the Key Distribution Center to **company.com**.
- **show active-directory all**
  Displays a list of all AAA Active Directory servers on the system.
- **delete active-directory MyActiveDirectoryServer**
  Deletes the AAA Active Directory server named **MyActiveDirectoryServer** from the system.

Options

- **admin-encrypted-password**
  Specifies the password associated with **admin name**. This option is required only when you are using an Active Directory Query agent with this Active Directory server object.
- **admin-name**
  Specifies the user name that has administrative permissions on an AAA Active Directory server. This option is required only when you are using an Active Directory Query agent with this Active Directory server object.
- **app-service**
  Specifies the name of the application service to which the object belongs. The default value is **none**. **Note:** If the **strict-updates** option is **enabled** on the application service that owns the object, you cannot modify or delete the object. Only the application service can modify or delete the object.
- **cleanup-cache**
  Specifies if this is a cache cleanup request. You can cleanup Group cache or PSO cache.
- **description**
  Specifies a description for the component. The default is **none**.

- **domain**
  Specifies the Active Directory domain name. This setting is required.
- **[name]**
  Specifies the name of an AAA Active Directory server. This setting is required.
- **domain-controller**
  Specifies the fully qualified domain name (FQDN) of the domain contoller for the domain specified in the **domain** option. The default is **none**.
- **domain-controllers**
  Adds, deletes, or replaces a set of domain controllers, by specifying an FQDN for each entry. You can configure the following options for each domain controller:
  - **ip**
    An IP address for specified domain controller entry.
- **group-cache-ttl**
  Specifies group cache lifetime in days [0..1825]. The default value is **30**. If you specify group cache lifetime 0, that means cache will be updated on every request.
- **pso-cache-ttl**
  Specifies password security objects (PSO) Cache lifetime in days [0..1825]. The default value is **30**. If you specify PSO cache lifetime 0, that means cache will be updated on every request.
- **location-specific**
  Specifies whether or not this object contains one or more attributes with values that are specific to the location where the BIG-IP device resides. The location-specific attribute is either true or false. When using policy sync, mark an object as location-specific to prevent errors that can occur when policies reference objects, such as authentication servers, that are specific to a certain location.
- **pool**
  Specifies the name of the pool with which the server is associated. The default is **none**.
- **partition**
  Displays the partition within which the component resides. The default is **Common**.
- **padata**
  Specifies a Kerberos preauthentication encryption type. If it is specified, the BIG-IP system includes Kerberos preauthentication data within the first AS-REQ. If you do not need to include preauthentication data, set this option to "none". Supported enctyption types: none, des-cbc-crc, des-cbc-md5, aes128-cts-hmac-sha1-96, aes256-cts-hmac-sha1-96, rc4-hmac. The default is **rc4-hmac**.
- **timeout**
  Specifies a timeout interval (in seconds) after which an AAA Active Directory server closes a connection. The default is **15**.

active-directory-trusted-domains

Manages authentication access policy (AAA) Active Directory® Trusted Domains.

Syntax

Configure the **active-directory-tusted-domains** component within the **aaa** module using the syntax shown in the following sections.

Create/Modify

```
create active-directory-trusted-domains [name]
modify active-directory-trusted-domains [name]
    app-service [[string] | none]
    root-domain [string]
    trusted-domains [add | delete | modify | replace-all-with] {
       {
         active-directory [name]
       }
    }
edit active-directory-trusted-domains [ [ [name] | [glob] | [regex] ] ... ]
    all-properties
    non-default-properties
```

Display

```
list active-directory-trusted-domains
list active-directory-trusted-domains [ [ [name] | [glob] | [regex] ] ... ]
show running-config active-directory-trusted-domains
show running-config active-directory-trusted-domains [ [ [name] | [glob] | [regex] ]
... ]
    all-properties
    app-service
    non-default-properties
    one-line
    partition
show active-directory-trusted-domains
show active-directory-trusted-domains [name]
```

Delete

```
delete active-directory-trusted-domains [name]
```

Description

You can use the **active-directory-trusted-domains** component to manage AAA Active Directory Trusted Domains. You can use this object to configure cross-domain authentication across a forest. It also allows to configure Active Directory® agents to work in a Route Domains environment.

Examples

- **create active-directory-trusted-domains MyTRD {**
  trusted-domains {
  myDomain1
  myDomain2
  myDomain3
  }
  root-domain /Common/myDomain2
  }
  Creates an object named **MyTRD**, sets domains myDomain1, myDomain2, myDomain3 as trusted and the root-domain is set to myDomain2. To use this example you need to have Active Directory servers myDomain1, myDomain2 and myDomain3 pre-configured.
- **show active-directory-trusted-domains all**
  Displays a list of all AAA Active Directory Trusted Domains on the system.
- **delete active-directory MyTRD**
  Deletes the AAA Active Directory Trusted Domains named **MyTRD** from the system.

Options

- **app-service**
  Specifies the name of the application service to which the object belongs. The default value is **none**. **Note:** If the **strict-updates** option is **enabled** on the application service that owns the object, you cannot modify or delete the object. Only the application service can modify or delete the object.
- **root-domain**
  Specifies an entry point to an Active Directory forest. An initial authentication request will always to be sent to root domain first. This setting is required.
- **trsuted-domains**
  Specifies a list of AAA Active Directory server components. Trust relationships should be defined for domains you add into this list. This setting is required.

See Also

active-directory

crldp

Configure a Certificate Revocation List Distribution Point (CRDLP) server object for implementing a CRLDP authentication module.

Syntax

Configure the **crldp** component within the **aaa** module using the syntax shown in the following sections.

Create/Modify

```
create crldp [name]
modify crldp [name]
    address [ip addr]
    allow-nullcrl [true | false]
    app-service [[string] | none]
    base-dn [[string> | none]
    cache-expire [[integer] | none]
    connection-timeout [[integer] | none]
    description [[string> | none]
    location-specific [true | false]
    pool [name]
    port [[integer] | none]
    reverse-dn [true | false]
    use-issuer [true | false]
    use-pool [enabled | disabled]
    verify-sig [true | false]
edit crldp | [glob] | [regex] ] ... ]
    all-properties
    non-default-properties
```

Display

```
list crldp
list crldp [ [ [name] | [glob] | [regex] ] ... ]
show running-config crldp
show running-config crldp [ [ [name] | [glob] | [regex] ] ... ]
    all-properties
    app-service
    non-default-properties
    one-line
    partition
show crldp
show crldp [name]
```

Delete

```
delete crldp [name]
```

Description

Configure a CRLDP authentication server, and then assign the server to the CRLDP auth agent in your access policy.

Examples

- **create crldp aaa-ldap-2027 { address 172.27.32.60 allow-nullcrl false base-dn DC=net,DC=aina,DC=test cache-expire 1000 connection-timeout 15 description none partition Common pool aaa-ldap-2027-pool port ldap reverse-dn true use-issuer false use-pool disabled verify-sig true }**
  Creates a CRLDP server named **aaa-ldap-2027**.
- **delete crldp server my_crldp_server**
  Deletes the CRLDP server named **my_crldp_server**.

Options

- **address**
  Specifies the IP address of the server. This option is required.
- **allow-nullcrl**
  Specifies whether to consider a null CRL from the CRLDP server a successful authentication. The default is **false**.
- **app-service**
  Specifies the name of the application service to which the object belongs. The default value is **none**. **Note:** If the **strict-updates** option is **enabled** on the application service that owns the object, you cannot modify or delete the object. Only the application service can modify or delete the object.
- **base-dn**
  Specifies the LDAP base directory name for certificates that specify the CRL distribution point in directory name (dirName) format. Used when the value of the X509v3 attribute crlDistributionPoints is of type dirName. In this case, the BIG-IP system attempts to match the value of the crlDistributionPoints attribute to the Base DN value. An example of a Base DN value is cn=lxxx,dc=f5,dc=com.
- **cache-expire**
  Specifies (in seconds) an update interval for CRL distribution points. The update interval for distribution points ensures that CRL status is checked at regular intervals, regardless of the CRL timeout value. This helps prevent CRL information from becoming outdated before the Access Policy Manager checks the status of a certificate.
- **connection-timeout**
  Specifies the number of seconds of inactivity the system allows before the connection times out. The default is **15**.
- **description**
  Specifies a unique description for the server. The default is **none**.

- **partition**
  Displays the partition within which the component resides.
- **location-specific**
  Specifies whether or not this object contains one or more attributes with values that are specific to the location where the BIG-IP device resides. The location-specific attribute is either true or false. When using policy sync, mark an object as location-specific to prevent errors that can occur when policies reference objects, such as authentication servers, that are specific to a certain location.
- **pool**
  Specifies the name of the pool with which the server is associated.
- **port**
  Specifies the CRLDP service port. The default is **389**.
- **reverse-dn**
  Specifies in which order the system is to attempt to match the Base DN value to the value of the X509v3 attribute crlDistributionPoints. Possible values are enabled and disabled. When set to enabled, the system matches the base DN from left to right, or from the beginning of the DN string, to accomodate dirName strings in certificates such as C=US,ST=WA,L=SEA,OU=F5,CN=xxx. The default value is **false**.
- **use-issuer**
  Specifies whether the CRL distribution point is extracted from the certificate of the client certificate issuer. The default is **false**.
- **use-pool**
  Enables or disables high availability between CRLDP servers. When **enabled**, Access Policy Manager sends CRLDP authentication requests for the associated CRLDP auth agent to the virtual server, and standard pool behavior is used to implement high availability for CRDLP.
- **verify-sig**
  Specifies whether the signature on the received CRL is verified. The default if **true**.

http

Specify an http server configuration used for authentication.

Syntax

Configure the **http** component within the **aaa** module using the syntax shown in the following sections.

Create/Modify

```
create http [name]
modify http [name]
    app-service [[string] | none]
    auth-type [form-based | basic-ntlm | custom-post]
    content-type [xml-utf8 | url-encoded-utf8 | none]
    custom-body [[string] | none]
    description [[string] | none]
    follow-redirect [integer]
    form-action [[string] | none]
    form-fields [[string] | none]
    form-method [get | post]
    form-params [[string] | none]
    form-password [[string] | none]
    form-username [[string] | none]
    headers [add | delete | modify | replace-all-with | none] {
        [name] {
            app-service [[string] | none]
            hname [[string] | none]
            hvalue [[string] | none]
        }
    }
    location-specific [true | false]
    start-uri [[string] | none]
    success-match-type [url | cookie | string | exact-cookie]
    success-match-value [[string] | none]
edit http [ [ [name] | [glob] | [regex] ] ... ]
    all-properties
    non-default-properties
```

Display

```
list http
list http [ [ [name] | [glob] | [regex] ] ... ]
show running-config http
show running-config http [ [ [name] | [glob] | [regex] ] ... ]
    all-properties
    app-service
    non-default-properties
    one-line
    partition
show http
show http [name]
```

Delete

```
delete http [name]
```

Description

You can use the **http** component to create and manage AAA HTTP servers.

Examples

- **create http myHttpServer {**
  start-uri "http://mycompany.com/" auth-type basic-ntlm }
  Creates an HTTP authentication server named "myHttpServer" with a starting URI of http://mycompany.com.
- **show http**
  Displays a list of AAA HTTP servers.
- **delete http myHttpServer**
  Deletes the **myHttpServer** AAA HTTP server.

Options

- **app-service**
  Specifies the name of the application service to which the object belongs. The default value is **none**. **Note:** If the **strict-updates** option is **enabled** on the application service that owns the object, you cannot modify or delete the object. Only the application service can modify or delete the object.
- **auth-type**
  Specifies the type of authentication you want to use.
  - **form-based**
    Specifies the authentication type to be form-based.
  - **basic-ntlm**
    Specifies the authentication type to be basic-ntlm.
  - **custom-post**
    Specifies the authentication type to be custom-post.
- **content-type**
  Specifies the encoding (xml-utf8, url-encoded-utf8, or none) for an HTTP custom post. If you specify ‘none’, you must use the headers option to add a custom header. In addition to specifying a custom header, you must apply your own encoding through an iRule.
- **custom-body**
  Specifies the body for a HTTP Custom Post.
- **description**
  Specifies a unique description for the server. The default is **none**.

- **follow-redirect**
  Specifies the number of pages away from the landing page the request should travel before failing.
- **form-action**
  Specifies the complete destination URL to process the form using HTTP form-based authentication. This is optional. If you do not specify a form action, then Access Policy Manager will use the URI from the request to perform HTTP form-based authentication.
- **form-fields**
  Specifies the hidden form parameters required by the authentication server logon form at your location. Refer to the *BIG-IP® Configuration Guide: Access Policy Manager®* for more information on how to determine hidden values.
- **form-method**
  Specifies the form method you want to use for the form-based HTTP authentication. The value is either Get or POST. The default is POST. However, if you specify GET, the Access Policy Manager will force the authentication using HTTP GET rather than perform authentication using form-based POST.
- **form-password**
  Specifies the parameter names used by the form you are sending the POST request to.
- **form-username**
  Specifies the parameter names used by the form you are sending the POST request to.
- **headers**
  Specifies the name and value of the header content to be inserted in an HTTP Post. The options are:
  - **app-service**
    Specifies the name of the application service to which the HTTP header belongs. The default value is **none**. **Note:** If the **strict-updates** option is **enabled** on the application service that owns the object, you cannot modify or delete the HTTP header. Only the application service can modify or delete the HTTP header.
  - **hname**
    The name of the HTTP header.
  - **hvalue**
    The value of the HTTP header.
- **location-specific**
  Specifies whether or not this object contains one or more attributes with values that are specific to the location where the BIG-IP device resides. The location-specific attribute is either true or false. When using policy sync, mark an object as location-specific to prevent errors that can occur when policies reference objects, such as authentication servers, that are specific to a certain location.
- **[name]**
  Specifies the name of the aaa http server. This option is required.

- **partition**
  Displays the partition within which the component resides. The default is **Common**.
- **start-uri**
  Specifies a URL resource, for example, http://plum.tree.lab2.sp.companynet.com/. This resource must respond with a challenge to a non-authenticated request.
- **success-match-type**
  Specifies the method your authentication server uses and determines the option definition used for this field. The field toggles according to your selection.
  - **cookie**
    Specifies any string in cookie is required.
  - **exact-cookie**
    Specifies key fields in cookie is required.
  - **string**
    Specifies a specific string is required.
  - **url**
    Specifies a URL is required.
- **success-match-value**
  Specifies the URL, any string in cookie, exact cookie or specific string used for the specific success match type you see.

kerberos

Configures a Kerberos server.

Syntax

Configure the **kerberos** component within the **aaa** module using the syntax shown in the following sections.

Create/Modify

```
create kerberos [name]
modify kerberos [name]
  options
    auth-realm [[string] | none]
    app-service [[string] | none]
    keytab-file-obj [[string] | none]
    location-specific [true | false]
    service-name [[string] | none]
edit kerberos | [glob] | [regex] ] ... ]
    all-properties
    non-default-properties
```

Display

```
list kerberos
list kerberos [ [ [name] | [glob] | [regex] ] ... ]
show running-config kerberos
show running-config kerberos [ [ [name] | [glob] | [regex] ] ... ]
    all-properties
    app-service
    non-default-properties
    one-line
    partition
show kerberos
show kerberos [name]
```

Delete

```
delete kerberos [name]
```

Description

You can use the **kerberos** component to create and manage AAA Kerberos servers. Use the Kerberos authentication server to configure authentication for the Access Policy Manager. A client retrieves credentials from the domain controller and passes those credentials to the Access Policy Manager. Then Access Policy Manager uses the value in the **keytab-file-obj** option of the Kerberos AAA server object to verify the credentials. Access Policy Manager system does not have to reside in the domain.

Examples

- **delete kerberos my_kerberos**
  Deletes the server named my_kerberos.

Options

- **auth-realm**
  Specifies a Kerberos auth realm name (administrative name), such as **user@realm.com** to establish the boundaries within which an authentication server has the authority to authenticate a user, host, or service. Kerberos clients manually map DNS domain names to Kerberos realm names. This option is required.
- **app-service**
  Specifies the name of the application service to which the object belongs. The default value is **none**. **Note:** If the **strict-updates** option is **enabled** on the application service that owns the object, you cannot modify or delete the object. Only the application service can modify or delete the object.
- **keytab-file-obj**
  Specifies a keytab file that contains the keys (derived from the Kerberos password) that the server uses to authenticate the client. This option is required.
- **location-specific**
  Specifies whether or not this object contains one or more attributes with values that are specific to the location where the BIG-IP device resides. The location-specific attribute is either true or false. When using policy sync, mark an object as location-specific to prevent errors that can occur when policies reference objects, such as authentication servers, that are specific to a certain location.
- **[name]**
  Specifies the name of an AAA Kerberos server. This option is required.
- **partition**
  Displays the partition within which the component resides.
- **service-name**
  Specifies the Kerberos service name defined inside KDC in the format **service name/hostname@kerberosrealm**. This option is required, for example, **HTTP**.

kerberos-keytab-file

Manages a Kerberos keytab file.

Syntax

Configure the **kerberos-keytab-file** component within the **aaa** module using the syntax shown in the following sections.

Create/Modify

```
create kerberos-keytab-file [name]
modify kerberos-keytab-file [name]
    app-service [[string] | none]
    source-path [string]
edit kerberos-keytab-file | [glob] | [regex] ] ... ]
    all-properties
    non-default-properties
```

Display

```
list kerberos-keytab-file
list kerberos-keytab-file [ [ [name] | [glob] | [regex] ] ... ]
show running-config kerberos-keytab-file
show running-config kerberos-keytab-file [ [ [name] | [glob] | [regex] ] ... ]
    all-properties
    app-service
    non-default-properties
    one-line
    partition
show kerberos-keytab-file
show kerberos-keytab-file [name]
```

Delete

```
delete kerberos-keytab-file [name]
```

Description

You can use the **kerberos-keytab-file** component to create and manage a Kerberos Keytab file.

Examples

- **create kerberos-keytab-file my_keytab {**
  source-path file:/root/apmkeytab
  }

  Creates a Kerberos Keytab file name **my_keytab** located at **root/apmkeytab**.

- **show kerberos-keytab-file**
  Displays a list of Kerberos Keytab files.
- **delete kerberos-keytab-file my_keytab**
  Deletes the Kerberos Keytab file name **my_keytab**.

Options

- **app-service**
  Specifies the name of the application service to which the object belongs. The default value is **none**. **Note:** If the **strict-updates** option is **enabled** on the application service that owns the object, you cannot modify or delete the object. Only the application service can modify or delete the object.
- **source-path**
  Specifies the location of the Kerberos Keytab file.
- **partition**
  Displays the partition within which the component resides.

See Also

kerberos, *kerberos*

ldap

Manages an AAA LDAP server.

Syntax

Configure the **ldap** component within the **aaa** module using the syntax shown in the following sections.

Create/Modify

```
create ldap [name]
modify ldap [name]
    address [[ip addr] | none]
    admin-dn [[string] | none]
    admin-encrypted-password [[string] | none]
    app-service [[string] | none]
    base-dn [string]
    description [[string] | none]
    is-ldaps [false | true]
    location-specific [true | false]
    pool [name]
    port [[service] | none]
    schema-attr {
        group-member [[string] | none]
        group-member-value [[string] | none]
        group-memberof [[string] | none]
        group-object-class [[string]]
        user-memberof [[string] | none]
        user-object-class [string]
    }
    serverssl-profile [none | serverssl | serverssl-insecure-compatible |
wom-default-serverssl]
    timeout [integer]
    use-pool [enabled | disabled]
edit ldap [ [ [name] | [glob] | [regex] ] ... ]
    all-properties
    non-default-properties
```

Display

```
list ldap
list ldap [ [ [name] | [glob] | [regex] ] ... ]
show running-config ldap
show running-config ldap [ [ [name] | [glob] | [regex] ] ... ]
    all-properties
    app-service
    non-default-properties
    one-line
    partition
show ldap
show ldap [name]
```

Delete

```
delete ldap [name]
```

Description

You can use the **ldap** component to create and manage an AAA LDAP server.

Examples

- **create ldap MyLDAPserver {**
  address 172.30.6.144
  admin-dn
  "cn=administrator,cn=users,dc=company,dc=companynet,dc=com"
  admin-encrypted-password "!MyPassword"
  }
  Creates the AAA LDAP server named **MyLDAPserver** that is assigned the
  IP address **172.30.6.144** and the
  cn=administrator,cn=users,dc=company,dc=companynet,dc=com admin dn
  with a password of **!MyPassword**.
- **show ldap all**
  Displays a list of AAA LDAP servers.
- **delete ldap MyLDAPServer**
  Deletes the AAA LDAP server named **MyLDAPServer** from the system.

Options

- **address**
  Specifies the IP address of an AAA LDAP server. This option is required.
- **admin-dn**
  Specifies the Container Distinguished Name (DN) to use for authentication. This option is required.
- **admin-encrypted-password**
  Specifies the password for **admin name**. This option is required.
- **app-service**
  Specifies the name of the application service to which the object belongs. The default value is **none**. **Note:** If the **strict-updates** option is **enabled** on the application service that owns the object, you cannot modify or delete the object. Only the application service can modify or delete the object.

- **base-dn**
  Specifies the base DN from which to search. This search DN is used to search groups across a whole directory.
- **group-cache-ttl**
  Specifies a lifetime for the group cache (days).
- **cleanup-cache**
  Specifies whether cache invalidation is required. The default is **none**. The options are:
  - **none**
  - **group**
- **description**
  Specifies a unique description for the server. The default is **none**.
- **is-ldaps**
  Specifies whether to use the LDAPS protocol during authentication. If **true**, you must also specify the option **serverssl-profile**.
- **location-specific**
  Specifies whether or not this object contains one or more attributes with values that are specific to the location where the BIG-IP device resides. The location-specific attribute is either true or false. When using policy sync, mark an object as location-specific to prevent errors that can occur when policies reference objects, such as authentication servers, that are specific to a certain location.
- **[name]**
  Specifies the name of the AAA server. This option is required.
- **partition**
  Displays the partition within which the component resides.
- **pool**
  Specifies the name of the pool with which the server is associated. The default is **none**.
- **port**
  Specifies the port number of the AAA LDAP server. The default is ldap. This option is required.
- **schema-attr**
  Specifies LDAP schema-specific attribute names.
  - **user-object-class**The value of the objectClass attribute for a user object. The default is "user".
  - **user-memberof**If the user object maintains a group membership, you should specify the membership attribute name here. The default is "memberOf".
  - **group-object-class**The value of the objectClass attribute for a group object. The default is "group".

- **group-memberof**If the group object maintains a group membership in other groups, you should specify a membership attribute name here. The default is "memberOf".
- **group-member**If the group object maintains a list of users that belong to the group, you should specify the attribute here. The default is "member".
- **group-member-value**If the "group-member" attribute is specified, you should specify the attribute that is used to add users into a group. The default is "dn".

◆ **serverssl-profile**
Specifies the server side SSL profile. LDAPS is achieved by directing LDAP traffic over a virtual server that uses a server side SSL to communicate with the LDAP server.
The options are:

- **serverssl**
- **serverssl-insecure-compatible**
- **wom-default-serverssl**

◆ **timeout**
Specifies a timeout interval (in seconds) for the AAA server after which the server closes a connection. The default is **15**.

◆ **use-pool**
Enables or disables high availability between pool members. When enabled, the Access Policy Manager sends AAA requests for the associated policy item to the virtual server, and standard pool behavior is used to implement high availability for CRDLP.

oam

Manages an AAA Oracle Access Manager server.

Syntax

Configure the **oam** component within the **aaa** module using the syntax shown in the following sections.

Create/Modify

```
create oam [name]
modify oam [name]
    access-server-hostname [[string] | none]
    access-server-name [[string] | none]
    access-server-port [[integer] | none]
    access-server-retries [integer]
    accessgate-encrypted-password [[string] | none]
    accessgates [add | delete | modify | replace-all-with] {
      [name]
    }
    action [config-accessgate | noop]
    admin-id [[string] | none]
    admin-password [[string] | none]
    app-service [[string] | none]
    description [[string] | none]
    enable [false | true]
    global-access-protocol-passphrase [[string] | none]
    location-specific [true | false]
    transport-security-mode [cert | open | simple]
edit oam | [glob] | [regex] ] ... ]
    all-properties
    non-default-properties
```

Display

```
list oam
list oam [ [ [name] | [glob] | [regex] ] ... ]
show running-config oam
show running-config oam [ [ [name] | [glob] | [regex] ] ... ]
    all-properties
    app-service
    non-default-properties
    one-line
    partition
show oam
show oam [name]
```

Delete

```
delete oam [name]
```

Description

You can use the **oam** component to create and manage an AAA Oracle Access Manager server.

Examples

- **create oam oam10g {**
  access-server-hostname www.localcorp.biz
  access-server-name accessSrv1
  access-server-port 6021
  access-server-retries 0
  accessgates {
  oam10gwebgate1 {
  encrypted-password [string]
  }
  }
  admin-id firstname.lastname
  admin-password "[string]"
  global-access-protocol-passphrase "[string]"
  transport-security-mode simple
  }
  Creates the AAA OAM server named **oam10g** accessing the web gate **oam10gwebgate1** on
  the Access Server **accessSrv1** at host name **www.localcorp.biz** on port **6021**. The server retries connections zero times.
- **show aaa oam all**
  Displays a list of all AAA Oracle Access Manager servers on the system.
- **delete aaa oam MyOAMServer**
  Deletes the AAA Oracle Access Manager server named **MyOAMServer** from the system.

Options

- **access-server-hostname**
  Specifies the IP address or FQDN of the Oracle Access Manager server. This option is required.
- **access-server-name**
  Specifies the name of the Oracle Access Manager server. This option is required.
- **access-server-port**
  Specifies the port of the Oracle Access Manager server. The default is **6021**.
- **access-server-retries**
  Specify the number of times you want the access gate to attempt to connect to the Oracle Access Manager server when the **action** option is set to **config-accessgate**. The default is **0** (zero).

- **accessgates**
  Specifies the ID of the access gate or web gate on the OAM Server. The system supports the use of multiple access gates/web gates as long as they are from the same OAM server.
- **action**
  Specifies the Oracle Access Manager action type. Actions allow you to pass user profile information or to redirect the user's browser to another site. For more information on Actions, refer to the Access Administration Guide provided by Oracle. The options are:
  - **config-accessgate**
    Specifies that you want the system to use the configureAccessGate tool.
  - **noop**
    Specifies "no operation performed." This is the default.
- **admin-id**
  Specifies the administrator ID required by the Oracle Access Manager server. This option is required.
- **admin-password**
  Specifies the administrator password required by the Oracle Access Manager server. The default is **none**.
- **app-service**
  Specifies the name of the application service to which the object belongs. The default value is **none**. **Note:** If the **strict-updates** option is **enabled** on the application service that owns the object, you cannot modify or delete the object. Only the application service can modify or delete the object.
- **description**
  Specifies a unique description for the Oracle Access Manager server. The default is **none**.
- **enable**
  Specifies whether you want to enable the server. The default is **true**.
- **global-access-protocol-passphrase**
  Specifies a global passphrase for all Oracle components. The default is **none**.
- **location-specific**
  Specifies whether or not this object contains one or more attributes with values that are specific to the location where the BIG-IP device resides. The location-specific attribute is either true or false. When using policy sync, mark an object as location-specific to prevent errors that can occur when policies reference objects, such as authentication servers, that are specific to a certain location.
- **[name]**
  Specifies the name of an AAA Oracle Access Manager server. This setting is required.
- **transport-security-mode**
  Specifies the transport security level for the communication between Oracle components and Access Policy Manager. The options are:

- **open**
  Communication is not encrypted for protection. Use this mode when security is not an issue
- **simple**
  Communication is encrypted with Oracle Access Manager's internal CA. Simple mode encrypts communications using Transport Layer Security, RFC 2246 (TLS v1). This mode is less secure than Cert mode. Use this mode if you have some security concerns but do not want to manage your own CA.
- **cert**
  Communication is encrypted with an external CA. Use cert mode if you want different certificates on OAM servers and webgates and you have a trusted 3rd party CA. Oracle Access Manager components use X.509 digital certificates in PEM format only.

ocsp

Configure Online Certificate System Protocol (OCSP) responder objects.

Syntax

Configure the **ocsp** component within the **aaa** module using the syntax shown in the following sections.

Create/Modify

```
create ocsp [name]
modify ocsp [name]
    allow-certs [true | false]
    app-service [[string] | none]
    ca-file (<file name> | none)
    ca-path (<file name> | none)
    cert-id-digest (sha1 | md5)
    chain [true | false]
    check-certs [true | false]
    explicit-ocsp [true | false]
    ignore-aia [true | false]
    intern [true | false]
    location-specific [true | false]
    nonce [true | false]
    sign-digest (sha1 | md5)
    sign-key (<file name> | none)
    sign-key-passphrase (<string> | none)
    sign-other (<file name> | none)
    signer (<file name> | none)
    status-age <number>
    trust-other [true | false]
    url (<string> | none)
    va-file (<file name> | none)
    validity-period <number>
    verify [true | false]
    verify-cert [true | false]
    verify-other (<string> | none)
    verif-sig [true | false]
edit ocsp | [glob] | [regex] ] ... ]
    all-properties
    non-default-properties
```

Display

```
list ocsp
list ocsp [ [ [name] | [glob] | [regex] ] ... ]
show running-config ocsp
show running-config ocsp [ [ [name] | [glob] | [regex] ] ... ]
    all-properties
    app-service
    non-default-properties
    one-line
    partition
show ocsp
show ocsp [name]
```

Delete

```
delete ocsp [name]
```

Description

To implement the SSL OCSP authentication module, create an OCSP responder object and assign it to the OCSP auth agent in your access policy.

Options

- **allow-certs**
  Specifies whether the addition of certificates to an OCSP request is enabled. The default is **true**.
- **app-service**
  Specifies the name of the application service to which the object belongs. The default value is **none**. **Note:** If the **strict-updates** option is **enabled** on the application service that owns the object, you cannot modify or delete the object. Only the application service can modify or delete the object.
- **ca-file**
  Specifies the name of the certificate file object containing trusted CA certificates used to verify the signature on the OCSP response. The default is **none**.
- **ca-path**
  Specifies the path to the trusted CA certificates used to verify the signature on the OCSP response. The default is **none**.
- **cert-id-digest**
  The cert ID digest is part of the OCSP protocol. The OCSP client (in this case, the BIG-IP system) calculates the cert ID using a hash of the Issuer and serial number for the certificate that it is trying to verify. The options are:
  - **sha1**
    Newer algorithm that provides a higher security level with a 160 bit hash length. This is the default.
  - **md5**
    Older algorithm with a 128 bit hash length.
- **chain**
  Specifies whether the system constructs a chain from certificates in the OCSP response. The default is **true**.
- **check-certs**
  Specifies whether the LTM system makes additional checks to see if the signer's certificate is authorized to provide the necessary status information. Use this option only for testing purposes. The default is **true**.

- **explicit-ocsp**
  Specifies whether the BIG-IP system explicitly trusts that the OCSP response signer's certificate is authorized for OCSP response signing. If the signer's certificate does not contain the OCSP signing extension, setting this option to **true** causes a response to be untrusted. The default is **true**.
- **ignore-aia**
  Specifies whether to ignore the URL contained in the certificate's AIA fields, and to always use the URL specified by the responder instead. The default is **false**.
- **intern**
  Specifies whether to ignore certificates contained in an OCSP response when searching for the signer's certificate. When you set this option to **true**, you must also specify the signer's certificate using either the **verify-other** or **va-file** option. The default is **true**.
- **location-specific**
  Specifies whether or not this object contains one or more attributes with values that are specific to the location where the BIG-IP device resides. The location-specific attribute is either true or false. When using policy sync, mark an object as location-specific to prevent errors that can occur when policies reference objects, such as authentication servers, that are specific to a certain location.
- **[name]**
  Specifies a unique name for the component. This option is required.
- **nonce**
  Specifies whether a nonce will be sent in an OCSP request. When set to **false**, the request is sent without a nonce. The default is **true**.
- **partition**
  Displays the partition within which the OCSP responder object resides.
- **sign-digest**
  Specifies the algorithm (md5 or sha1> used to sign a request using a signing certificate and key. The default is **sha1**. If you use this option, you must also set the **sign-key** and **sign-key-passphrase** options.
- **sign-key**
  Specifies the key used to sign an OCSP request. If you use this option, you must also set the **sign-digest** and **sign-key-passphrase** options. The default is **none**.
- **sign-key-passphrase**
  Specifies the passphrase for the signing key. If you use this option, you must also set the **sign-digest** and **sign-key** options. The default is **none**.
- **sign-other**
  Specifies additional certificates to add to an OCSP request. The options are **default.crt** and **ca-bundle.crt**. The default is **none**.
- **signer**
  Specifies the certificate used to sign an OCSP request. If the certificate is specified but the key is not specified, then the private key is read from the same file as the certificate. If neither the certificate nor the key is

specified, then the request is not signed. If the certificate is not specified and the key is specified, then the configuration is considered to be invalid. The default is **none**.

- **status-age**
  Species the amount of time (in seconds) to compare to the **notBefore** value of a status response. Use this option only when a status response does not include the **notAfter** field. The default is **0** (zero).
- **trust-other**
  Specifies whether the BIG-IP system trusts the certificates specified using the **verify-other** option. The default is **false**.
- **url**
  Specifies the URL used to contact the OCSP service on the responder. This option is required. The default is **none**.
- **va-file**
  Specifies the name of the file containing explicitly-trusted responder certificates. Use this option when the responder is not covered by the certificates already loaded into the responder's CA store. The default is **none**.
- **validity-period**
  Specifies an acceptable error range in seconds. Use this option when the OCSP responder clock and a client clock are not synchronized, which could cause a certificate status check to fail. This value must be a positive number. This option is required. The default is **300**.
- **verify**
  Specifies whether verification of an OCSP response signature or the nonce values is enabled. Use this option only for debugging purposes. The default is **true**.
- **verify-cert**
  Specifies whether the BIG-IP system verifies the certificate in the OCSP response. The default is **true**.
- **verify-other**
  Specifies the name of the file used to search for an OCSP response signing certificate when the certificate has been omitted from the response. The default is **none**.
- **verify-sig**
  Specifies whether the BIG-IP system checks the signature on the OCSP response. Use this option only for testing purposes. The default is **true**.

radius

Manages an AAA RADIUS server.

Syntax

Configure the **radius** component within the **aaa** module using the syntax shown in the following sections.

Create/Modify

```
create radius [name]
modify radius [name]
     acct-port [integer]
     address [[ip addr] | none]
     auth-port [integer]
     app-service [[string] | none]
     description [[string] | none]
     mode [acct | auth | both | none]
     nas-ip-address [[ip addr] | none]
     nas-ipv6-address [[ip addr] | none]
     pool [[string] | none]
     retries [integer]
     secret [string]
     service-type [default | login | framed | callback-login | callback-framed |
outbound | administrative | nas-prompt | authenticate-only | callback-nas-promit |
call-check | callback-administrative]
     timeout [[integer] | immediate | indefinite]
     use-pool [enabled | disabled]
edit radius | [glob] | [regex] ] ... ]
    all-properties
    non-default-properties
```

Display

```
list radius
list radius [ [ [name] | [glob] | [regex] ] ... ]
show running-config radius
show running-config radius [ [ [name] | [glob] | [regex] ] ... ]
    all-properties
    app-service
    non-default-properties
    one-line
    partition
show radius
show radius [name]
```

Delete

```
delete radius [name]
```

Description

You can use the **radius** component to create and manage an AAA RADIUS server.

Examples

- **create rad_auth {**
  address 172.30.6.144
  secret "test"
  use-pool "disabled"
  }
  Creates the AAA RADIUS server named **rad_auth** that has an IP address of **172.30.6.144** and has a shared secret of **test**.
- **show radius all**
  Displays a list of all AAA RADIUS servers on the system.
- **delete radius MyRadiusServer**
  Deletes the AAA RADIUS server named **MyRadiusServer** from the system.

Options

- **acct-port**
  Specifies the port number of the external AAA RADIUS accounting server. The default is **radius-acct**.
- **address**
  Specifies the IP address of the AAA RADIUS server. This option is required.
- **auth-port**
  Specifies the port number for the service. The default is **radius**. This option is required.
- **app-service**
  Specifies the name of the application service to which the object belongs. The default value is **none**. **Note:** If the **strict-updates** option is **enabled** on the application service that owns the object, you cannot modify or delete the object. Only the application service can modify or delete the object.
- **description**
  Specifies a unique description for the AAA RADIUS server. The default is **none**.
- **mode**
  Specifies the configuration mode you want to use for RADIUS authentication. Note that you cannot modify the mode once you create the server. The options are:

- **acct**
  Configures the system to perform only RADIUS accounting. Use this option to pass accounting information about your users to the external RADIUS accounting server.
- **auth**
  Configures the system to perform only RADIUS authentication. Use this option to authenticate your users through a RADIUS server.
- **both**
  Configures the system to perform both RADIUS authentication and RADIUS accounting simultaneously.
- **none**
  Configures the system to perform neither RADIUS authentication nor RADIUS accounting.

◆ **[name]**
Specifies the name of an AAA RADIUS server. This option is required.

◆ **nas-ip-address**
Specifies an IP address as RADIUS attribute 4 that you can configure without changing the source IP address in the IP header of the RADIUS packets. Use this option in situations where you are using an NAS cluster to be recognized as a single RADIUS client.

◆ **nas-ipv6-address**
Specifies an IPv6 address as RADIUS attribute 4 that you can configure without changing the source IP address in the IP header of the RADIUS packets. Use this option in situations where you are using an NAS cluster to be recognized as a single RADIUS client.

◆ **partition**
Displays the partition within which the component resides.

◆ **pool**
Specifies the name of the pool to which this server belongs. The default is **none**.

◆ **retries**
Specifies the number of times the BIG-IP system tries to make a connection to the RADIUS AAA server after the first attempt fails. The default is **3**.

◆ **secret**
Specifies the shared secret password of the AAA RADIUS server. This option is required.

◆ **service-type**
Specifies the type of service used for the RADIUS server. The default is **default**, which behaves as **authenticate-only**.

◆ **timeout**
Specifies a timeout interval (in seconds) for the AAA RADIUS server after which the server closes a connection. The default is **5**.

◆ **use-pool**
Enables or disables the use of the pool specified using the **pool** option. The default is **none**.

saml

Specify a SAML server configuration used for authentication.

Syntax

Configure the **saml** component within the **aaa** module using the syntax shown in the following sections.

Create/Modify

```
create saml [name]
modify saml [name]
    app-service [[string] | none]
    assertion-consumer-binding [http-artifact | http-post]
    description [[string] | none]
    entity-id [string]
    export-metadata [ no-signing | with-signing ]
    idp-connectors [add | delete | modify | none | replace-all-with] {
      [name] {
        idp-matching-source [[string] | none]
        idp-matching-value [[string] | none]
      }
    }
    is-authn-request-signed [true | false]
    location-specific [true | false]
    metadata-cert [[string] | none]
    metadata-file [[string] | none]
    metadata-signkey [[string] | none]
    relay-state [[string] | none]
    sp-certificate [[string] | none]
    sp-signkey [[string] | none]
    want-assertion-encrypted [true | false]
    want-assertion-signed [true | false]
edit saml [ [ [name] | [glob] | [regex] ] ... ]
    all-properties
    non-default-properties
```

Display

```
list saml
list saml [ [ [name] | [glob] | [regex] ] ... ]
show running-config saml
show running-config saml [ [ [name] | [glob] | [regex] ] ... ]
    all-properties
    app-service
    non-default-properties
    one-line
    partition
```

Delete

```
delete saml [name]
```

Description

You can use the **saml** component to create and manage saml aaa servers.

Examples

- **create saml my_saml_server { entity-id "https://spvs1.mycompany.com/id" want-assertion-signed true want-assertion-encrypted false is-authn-request-signed true sp-certificate my_company.crt sp-signkey my_company.key}**
  Creates a SAML authentication server named **my_saml_server** with certificate my_company.crt and key my_company.key and security options requiring signed assertion and want to send signed authentication request.
- **list saml**
  Displays a list of aaa saml servers.
- **delete saml my_saml_server**
  Deletes the **my_saml_server** aaa saml server.

Options

- **app-service**
  Specifies the name of the application service to which the object belongs. The default value is **none**. **Note:** If the **strict-updates** option is **enabled** on the application service that owns the object, you cannot modify or delete the object. Only the application service can modify or delete the object.
- **assertion-consumer-binding**
  Specifies method this BIG-IP as SP uses to receive assertions. Default value is **http-post**.
- **description**
  Specifies a unique description for the server. The default is **none**.
- **entity-id**
  In the entity-id field, type a unique identifier for the SP that is a URI that points to the BIG-IP virtual server which is going to act as a SAML service provider. For example, "https://www.mycompany-sp.com" points to the virtual server you use for BIG-IP as a SAML SP.
- **export-metadata**
  You can simplify SAML configuration using metadata files. When you use BIG-IP as an SP, you can export metadata for an SP to a file. Then you can use the file to configure SP metadata on an IdP system by importing the file or using the information in the file to configure the SP. You can choose to sign metadata while exporting it for better security. For example:
  1. Exporting metadata with signing. This requires metadata-cert and metadata-signkey files.
  modify saml aaa_obj {export-metadata with-signing

```
metadata-file /shared/sp_signed_metadata.xml
metadata-cert default.crt metadata-signkey
default.key}
```

2. Exporting metadata with no signing.

```
modify saml aaa_obj {export-metadata no-signing
metadata-file /shared/sp_metadata.xml}
```

- **idp-connectors**
  Add one or more IdP connectors to this SP service. BIG-IP SP redirect users to associated IdPs for authentication. If more IdP connectors associated with the SP, BIG-IP SP selects one of the IdP based on the specified selection criteria.
  For example:
  1. The following command associates one IdP connect to an SP

```
modify saml my_saml_server idp-connectors add {
my_idp_connector1 }
```

  2. Following associates multiple IdP connectors to SP with selection criteria based on landing URI. If the landing URI is /google, the user is sent to IdP as specified by my_idp_connector_google_app and if the landing URI is /salesforce, the user is sent to IdP as specified by my_idp_connector_for_salesforce.

```
modify saml my_saml_server idp-connectors add {
my_idp_connector_google_app { idp-matching-source
"%{session.server.landinguri}" idp-matching-value
"/*google" } my_idp_connector_for_salesforce {
idp-matching-source "%{session.server.landinguri}"
idp-matching-value "/salesforce"}}
```

- **is-authn-request-signed**
  This property specifies whether the SP signs authentication requests while sending them to the IdP. Set it to true if this BIG-IP SP should sign authentication requests. The default value for this is **false**.
- **location-specific**
  Objects of this class might have location specific attributes. Admin can indicate if object is location specific by setting it to true.
- **metadata-cert**
  Specifies the certificate with public key of the key pair used in signing the metadata. See export-metadata for more information on metadata export functionality. This is the certificate to be included in signed metadata when we export metadata. This might or might not be SP certificate.
- **metadata-file**
  Specifies the file to which metadata is saved. See export-metadata for more information on metadata export functionality.
- **metadata-signkey**
  Specifies the key that is used to sign SP's metadata. See export-metadata for more information on metadata export functionality.

- **relay-state**
  Specifies the value where the BIG-IP as SP redirects users after they are successfully authenticated and have been allowed by access policy. When BIG-IP receives the relay state from the IdP in addition to assertion, then it uses the value received from IdP to redirect the user to after authentication. Otherwise, BIG-IP uses the value from this configuration.
- **sp-certificate**
  BIG-IP includes this certificate in the SAML SP metadata that you export. After the SAML SP metadata is imported on the IdP, the IdP can use this certificate to verify signed authentication request and to encrypt assertion.
- **sp-signkey**
  This specifies the private key used to sign authentication requests if "is-authn-request-signed property" is set to true or to decrypt assertions when "want-assertion-encrypted" is set to true.
- **want-assertion-encrypted**
  This property specifies whether SP requires encrypted assertions. Set it to true if this BIG-IP SP requires encrypted assertions from the SAML IdP. The default value for this is false.
- **want-assertion-signed**
  This property specifies whether SP requires signed assertions. Set it to true if this BIG-IP SP requires signed assertions from the SAML IdP. The default value for this is true.

saml-idp-connector

Specify saml idp connector configuration used for SAML authentication.

Syntax

Configure the **saml-idp-connector** component within the **aaa** module using the syntax shown in the following sections.

Create/Modify

```
create saml-idp-connector [name]
modify saml-idp-connector [name]
    app-service [[string] | none]
    artifact-resolution-service-addr [IP address]
    artifact-resolution-service-port [integer]
    artifact-resolution-service-url [[string] | none]
    basic-auth-password [[string] | none]
    basic-auth-username [[string] | none]
    description [[string] | none]
    entity-id [string]
    identity-location [attribute | subject]
    identity-location-attribute [[string] | none]
    idp-certificate [[string] | none]
    import-metadata [[metadata-file] | none]
    location-specific [ true | false ]
    metadata-cert [[string] | none]
    serverssl-profile-name [profile name | none]
    sign-artifact-resolution-rq [true | false]
    sso-binding [http-post | http-redirect]
    sso-uri [[string] | none]
    want-authn-request-signed [true | false]
edit saml-idp-connector [ [ [name] | [glob] | [regex] ] ... ]
    all-properties
    non-default-properties
```

Display

```
list saml-idp-connector
list saml-idp-connector [ [ [name] | [glob] | [regex] ] ... ]
show running-config saml-idp-connector
show running-config saml-idp-connector [ [ [name] | [glob] | [regex] ] ... ]
    all-properties
    app-service
    non-default-properties
    one-line
    partition
```

Delete

```
delete saml-idp-connector [name]
```

Description

You can use the **saml-idp-connector** to create and manage saml idp connectors.

Examples

- **create saml-idp-connector my_idp_connector { import-metadata /shared/tmp/meta_data_idp.xml}**
  Creates saml idp connector named **my_idp_connector** from metadata. In this example "/shared/tmp/meta_data_idp.xml" is a file containing saml identity provider metadata.
- **create saml-idp-connector my_idp_connector1 { entity-id "https://www.secureauth.com/dom1" identity-location subject sso-binding http-post sso-uri "https://www.secureauth.com/dom1/acs/" idp-certificate my_company.crt}**
  Creates a saml idp connector named **my_idp_connector1** with certificate "my_company.crt" with identity-location "subject".
- **list saml-idp-connector**
  Displays a list of saml idp connectors.
- **delete saml-idp-connector my_idp_connector**
  Deletes the **my_idp_connector** saml idp connector.

Options

- **app-service**
  Specifies the name of the application service to which the object belongs. The default value is **none**. **Note:** If the **strict-updates** option is **enabled** on the application service that owns the object, you cannot modify or delete the object. Only the application service can modify or delete the object.
- **artifact-resolution-service-addr**
  Specifies the IP address that this BIG-IP as SP will use to connect to the IdP artifact resolution service. Value must be a valid IPv4 or IPv6 address.
- **artifact-resolution-service-port**
  Specifies the port that this BIG-IP as SP will use to connect to the IdP artifact resolution service.
- **artifact-resolution-service-url**
  Specifies the URI of the IdP artifact resolution service. The URI must include protocol, hostname, and full path.
- **basic-auth-password**
  Specifies the password for basic authentication. When configured, basic authentication is used for the artifact resolve request sent to the IdP.

- **basic-auth-username**
  Specifies username for basic authentication. When configured, basic authentication is used for the artifact resolve request sent to the IdP.
- **description**
  Specifies a unique description for the saml idp connector. The default is **none**.
- **entity-id**
  Specifies unique URI to represent the IdP pointed by idp connector.
- **identity-location**
  Specifies location of user identity inside SAML assertion. It can be either one of the attributes or the subject.
- **identity-location-attribute**
  If the location of user identity is set to attribute then attribute name should be specified as part of this attribute.
- **idp-certificate**
  This is IdP's certificate and is used by BIG-IP as SP to verify the signature of the assertion.
- **import-metadata**
  This attribute specifies the metadata file from an external IdP system used for creating idp connector object.
  For example: **create saml-idp-connector my_idp_connector { import-metadata /shared/tmp/meta_data_idp.xml}**
- **location-specific**
  Objects of this class might have location specific attribute(s). Admin can indicate if object is location specific by setting it to true.
- **metadata-cert**
  This specifies the certificate to use to verify the signature of metadata imported from a file.
  For example: **create saml-idp-connector my_idp_connector2 {import-metadata /shared/tmp/meta_data_signed_idp.xml metadata-cert default.crt}**
- **serverssl-profile-name**
  Specifies the SSL profile used when this BIG-IP as SP connects to the IdP artifact resolution service.
- **sign-artifact-resolution-rq**
  Specifies whether the IdP requires artifact resolve requests to be signed. Default value is true.
- **sso-binding**
  This specifies the method the IdP uses to receive authentication request from BIG-IP as SP. Default value is **http-post**
- **sso-uri**
  This specifies the URL of IdP's SSO service where BIG-IP as SP sends an authentication request to IdP.
- **want-authn-request-signed**
  This property specifies whether IdP requires signed authentication request. Set it to true if this BIG-IP as SP is required to send signed authentication request to IdP. The default value for this attributes is false.

securid

Manages an RSA SecurID authentication server.

Syntax

Configure the **securid** component within the **aaa** module using the syntax shown in the following sections.

Create/Modify

```
create securid [name]
modify securid [name]
    app-service [[string] | none]
    config-files [[string]| none]
    description [[string]| none]
    location-specific [true | false]
    source-ip [ip addr]
edit securid | [glob] | [regex] ] ... ]
    all-properties
    non-default-properties
```

Display

```
list securid
list securid [ [ [name] | [glob] | [regex] ] ... ]
show running-config securid
show running-config securid [ [ [name] | [glob] | [regex] ] ... ]
    all-properties
    app-service
    non-default-properties
    one-line
    partition
show securid
show securid [name]
```

Delete

```
delete securid [name]
```

Description

You can use the **securid** component to create and manage an RSA SecurID authentication server.

Examples

- **create securid mySecuridServer {**
  config-files add {
  sdconf.rec {

```
    local-path /shared/tmp/1
   }
  }
  source-ip 172.31.54.138
 }
```

Creates the **mySecuridServer** AAA RSA SecurID server.

- **list securid all**
  Displays a list of AAA RSA SecurID servers on the system.
- **delete securid mySecuridServer**
  Deletes the **mySecuridServer** AAA RSA SecurID server from the system.

Options

- **app-service**
  Specifies the name of the application service to which the object belongs. The default value is **none**. **Note:** If the **strict-updates** option is **enabled** on the application service that owns the object, you cannot modify or delete the object. Only the application service can modify or delete the object.
- **config-files**
  Specifies which files to use for SecurID authentication. Upload a copy of the **sdconf.rec** file from your RSA Authentication Manager server.
- **description**
  Specifies a description for the configuration file you are uploading.
- **location-specific**
  Specifies whether or not this object contains one or more attributes with values that are specific to the location where the BIG-IP device resides. The location-specific attribute is either true or false. When using policy sync, mark an object as location-specific to prevent errors that can occur when policies reference objects, such as authentication servers, that are specific to a certain location.
- **source-ip**
  Specifies the source IP address of the RSA SecurID agent. This option is required when authenticating to the RSA Authentication Manager server.
- **partition**
  Displays the partition within which the component resides.

tacacsplus

Configure a TACACS+ server for implementing remote TACACS+-based client authentication.

Syntax

Configure the **tacacsplus** component within the **apm aaa** module using the syntax shown in the following sections.

Create/Modify

```
create tacacsplus
modify tacacsplus
    address [ip addr]
    auth-service [arap | enable | fwproxy | login | nasi | none | ppp | pt | rcmd |
x25]
    auth-type [arap | ascii | chap | mschap | pap]
    app-service [[string] | none]
    description [[string]| none]
    encrypt [enabled | disabled]
    location-specific [true | false]
    pool [[string]| none]
    port [[string]| none]
    priv-lvl [max | min | user]
    protocol [atalk | deccp | ftp | http | ip | ipx | lat | lcp | osicp | pad | rlogin
| telnet | tn3270 | unknown | vines | vpdn | xremote]
    secret [[string]| none]
    service [none | arap | connection | firewall | ppp | shell | slip | system |
tty-daemon]
    use-pool [[string]| none]
edit tacacsplus | [glob] | [regex] ] ... ]
    all-properties
    non-default-properties
```

Display

```
list tacacsplus
list tacacsplus [ [ [name] | [glob] | [regex] ] ... ]
show running-config tacacsplus
show running-config tacacsplus [ [ [name] | [glob] | [regex] ] ... ]
    all-properties
    app-service
    non-default-properties
    one-line
    partition
show tacacsplus
show tacacsplus [name]
```

Delete

```
delete tacacsplus [name]
```

Description

You can use the **tacacsplus** component to create and manage a TACACS+ authentication server.

Examples

- **create tacacsplus mytacacs auth-service enable encrypt enabled**
  Creates a TACACS server named **mytacacs** with encryption enabled.

Options

- **address**
  Specifies the IP address of the TACACS+ server. This option is required.
- **auth-service**
  Specifies the name of the service that the user is requesting to be authenticated to use. This enables the TACACS+ server to behave differently for different types of authentication requests. This option is required.
- **auth-type**
  Specifies the type of authentication to be used for authenticating the user.
- **app-service**
  Specifies the name of the application service to which the object belongs. The default value is **none**. **Note:** If the **strict-updates** option is **enabled** on the application service that owns the object, you cannot modify or delete the object. Only the application service can modify or delete the object.
- **description**
  Specifies a unique description for the component. The default is **none**.
- **encrypt**
  Enables or disables encryption of TACACS+ packets. Recommended for normal use. The default is **enabled**.
- **location-specific**
  Specifies whether or not this object contains one or more attributes with values that are specific to the location where the BIG-IP device resides. The location-specific attribute is either true or false. When using policy sync, mark an object as location-specific to prevent errors that can occur when policies reference objects, such as authentication servers, that are specific to a certain location.
- **[name]**
  Specifies the name of an AAA TACACS+ server. This option is required.
- **partition**
  Displays the partition within which the component resides.

- **pool**
  Specifies the name of the pool to which this server belongs. The default is **none**.
- **port**
  Specifies the port number of the server. The default is **49**.
- **priv-lvl**
  Specifies the privilege level at which the user is authenticating. The options are:
  - **max**
  - **min**
    This is the default.
  - **user**
- **protocol**
  Specifies the protocol associated with the value specified in the service option, which is a subset of the associated service being used for client authorization or system accounting. The default is **unknown**.
- **secret**
  Sets the secret key used to encrypt and decrypt packets sent or received from the server. This option is required.
- **service**
- **use-pool**
  Enables or disables the use of the pool specified using the **pool** option. The default is **none**.

30

apm epsec

- Introducing the apm epsec module
- Alphabetical list of components

Introducing the apm epsec module

You can use the tmsh components that reside within the apm epsec module to configure BIG-IP® Access Policy Manager®. For more information about the tmsh hierarchical structure, see Chapter 2, *Understanding and Using the Traffic Management Shell*.

Alphabetical list of components

The remainder of this chapter lists the tmsh components that are available in the apm epsec module.

epsec-package

Manages an EPSEC package.

Syntax

Configure the **epsec-package** component within the **apm epsec** module using the syntax shown in the following sections.

Create

```
create epsec-package
    local-path [string]
    server [[string] | none]
```

Display

```
list epsec-package
    all-properties
    non-default-properties
    recursive
list epsec-package [name]
```

Install

```
install epsec-package [name]
    device-group [string]
```

Delete

```
delete epsec-package [name]
```

Description

You can use the **epsec-package** component to create, install and manage an EPSEC package.

Examples

- **create epsec-package my_epsec_package local-path /tmp/my_epsec_package**
  Creates an EPSEC package named **my_epsec_package** under the /Common/EPSEC/Upload folder.
- **list epsec-package**
  Displays a list of EPSEC packages under the specific folder. To list all EPSEC pacakges use the recursive option.

- **install epsec-package my_epsec_package**
  Installs the EPSEC package named **my_epsec_package** on this device.
- **install epsec-package my_epsec_package device-group /Common/my_epsec_dg**
  Installs the EPSEC package named **my_epsec_package** on the devices in the device group /Common/my_epsec_dg.
- **delete epsec-package my_epsec_package**
  Deletes the EPSEC package named **my_epsec_package**.

Options

- **[name]**
  Specifies the name of the component. This option is required.
- **local-path**
  Specifies the local path of the package to be uploaded. This option is valid only with CREATE command and is a required option.
- **device-group**
  Specifies the device group on which the package will be installed. This option is valid only with INSTALL command

software-status

Displays the status of the EPSEC software installation.

Syntax

Display information about the **software-status** component within the **apm epsec** module using the following syntax.

Display

```
show software-status
```

Description

You can use the **software-status** component to display the status of the EPSEC software installation, including the version of the EPSEC package being installed and the OESIS software version.

Examples

show software-status

Displays the status of the EPSEC software installation in a table.

See Also

epsec-package

31

apm mam

- Introducing the apm mam module
- Alphabetical list of components

Introducing the apm mam module

You can use the tmsh components that reside within this module to configure a MAM server for Mobile Applications.

For more information about the tmsh hierarchical structure, see Chapter 2, *Understanding and Using the Traffic Management Shell*.

Alphabetical list of components

The remainder of this chapter lists the tmsh components that are available in the apm mam module.

idbridge

Specify an IDBridge profile to be used for MAM Server.

Syntax

Configure the **idbridge** profile within the **mam** module using the syntax shown in the following sections.

Create/Modify

```
create idbridge [name]
   app-service [[string] | none]
   description [[string] | none]
   location-specific[true | false]
   mam-server [string]
   scim-config [string]
modify idbridge [name]
   app-service [[string] | none]
   description [[string] | none]
   location-specific[true | false]
   mam-server [string]
   scim-config [string]
```

Display

```
list idbridge
list idbridge [ [ [name] | [glob] | [regex] ] ... ]
show running-config idbridge
show running-config idbridge [ [ [name] | [glob] | [regex] ] ... ]
    all-properties
    app-service
    non-default-properties
    one-line
    partition
```

Delete

```
delete idbridge [name]
```

Description

You can use the **idbridge** component to create and manage ID Bridge profile for MAM Server.

Examples

- **create idbridge myIdBridge mam-server myMamServer scim-config myScimConfig**
  Creates an IdBridge profile named "myIdBridge" attached to myMamServer and myScimConfig.
- **show idbridge**
  Displays a list of IdBridge profiles.
- **delete idbridge myIdBridge**
  Deletes the **myIdBridge** profile.

Options

- **app-service**
  Specifies the name of the application service to which the object belongs. The default value is **none**. **Note:** If the **strict-updates** option is **enabled** on the application service that owns the object, you cannot modify or delete the object. Only the application service can modify or delete the object.
- **mam-server**
  Specifies the mam-server use attach this profile.
- **scim-config**
  Specifies the SCIM Config the profile uses.
- **description**
  Specifies a unique description for the server. The default is **none**.
- **app-service**
  Specifies the name of the application service to which the object belongs. The default value is **none**. **Note:** If the **strict-updates** option is **enabled** on the application service that owns the object, you cannot modify or delete the object. Only the application service can modify or delete the object.
- **location-specific**
  Specifies whether or not this object contains one or more attributes with values that are specific to the location where the BIG-IP device resides. The location-specific attribute is either true or false. When using policy sync, mark an object as location-specific to prevent errors that can occur when policies reference objects, such as authentication servers, that are specific to a certain location.
- **[name]**
  Specifies the name of the idbridge profile. This option is required.
- **partition**
  Displays the partition within which the component resides. The default is **Common**.

mam-server

Specify an MAM server configuration used for Mobile Applications.

Syntax

Configure the **mam-server** component within the **mam** module using the syntax shown in the following sections.

Create/Modify

```
create mam-server [name]
modify mam-server [name]
   address [ip-address]
   app-service [[string] | none]
   callback-path [string]
   callback-url [complete-url]
   description [[string] | none]
   encryption-key [[string] | none]
   fqdn [string]
   pool-name [string | none]
   port [string]
   serverssl-profile [none | profile name]
   use-pool enabled
edit mam-server [ [ [name] | [glob] | [regex] ] ... ]
    all-properties
    non-default-properties
```

Display

```
list mam-server
list mam-server [ [ [name] | [glob] | [regex] ] ... ]
show running-config mam-server
show running-config mam-server [ [ [name] | [glob] | [regex] ] ... ]
    all-properties
    app-service
    non-default-properties
    one-line
    partition
```

Delete

```
delete mam-server [name]
```

Description

You can use the **mam-server** component to create and manage MAM server.

Examples

- **create serv1 fqdn mymam.com serverssl-profile mySSlProfile callback-url http://mybigIP.com/asg address A.B.C.D**
  Creates an MAM server named "serv1" with a FQDN of mymam.com
- **list mam-server**
  Displays a list of MAM servers.
- **delete mam-server serv1**
  Deletes the **serv1** MAM server.

Options

- **app-service**
  Specifies the name of the application service to which the object belongs. The default value is **none**. **Note:** If the **strict-updates** option is **enabled** on the application service that owns the object, you cannot modify or delete the object. Only the application service can modify or delete the object.
- **server-ssl**
  Specifies the server SSL profile the system uses to connect to this remote endpoint. This setting overrides the **server-ssl** setting for the **local-endpoint** component. The default value is **none**.
- **fqdn**
  Specifies the FQDN of MAM Server.
- **port**
  Specifies the port of MAM Server.
- **pool-name**
  Specifies the pool-name for MAM Server.
  - **[name]**
    Specifies the name of the MAM server. This option is required.
  - **partition**
    Displays the partition within which the component resides. The default is **Common**.
  - **callback-path**
    Specifies a URL resource. This resource is the callback URI used in callback-path.
  - **callback-url**
    Specifies a URL resource. This resource is the callback URL for MAM Server to callback BIGIP/APM.

32

apm mam scim-config

- Introducing the apm mam scim-config module
- Alphabetical list of components

Introducing the apm mam scim-config module

You can use the tmsh components that reside within the apm mam scim-config module to configure SCIM configuration for a Mobile Access (MAM) server.

For more information about the tmsh hierarchical structure, see Chapter 2, *Understanding and Using the Traffic Management Shell*.

Alphabetical list of components

The remainder of this chapter lists the tmsh components that are available in the apm mam scim-config module.

scim-config

Specify an scim configuration used by authentication as specified in idbridge profile.

Syntax

Configure the **scim-config** component within the **mam** module using the syntax shown in the following sections.

Create/Modify

```
create scim-config [name]
   app-service [[string] | none]
   auth-server [string]
   description [[string] | none]
   group-dn [string]
   group-obj-class [string]
   rdn-attr [string]
   user-dn [string]
   user-obj-class [string]
modify scim-config [name]
   auth-server [string]
   description [[string] | none]
   group-dn [string]
   group-obj-class [string]
   rdn-attr [string]
   user-dn [string]
   user-obj-class [string]
```

Display

```
list scim-config
list scim-config [ [ [name] | [glob] | [regex] ] ... ]
```

Delete

```
delete scim-config [name]
```

Description

You can use the **scim-config** component to create and manage SCIM-Configuration for LDAP Server interface.

Examples

- **create scim-config myScim create mySCIM auth-server hello group-dn CN=users,DC=adam,DC=lab,DC=fp,DC=f5net,DC=com group-obj-class group rdn-attr sAMAccountName user-dn**

sAMAccountName user-obj-class user
Creates a scim-config to be used for LDAP server by BIGIP for MAM, named "myScim".

- **list scim-config**
  Displays a list of scim config.
- **delete scim-config myScim**
  Deletes the **myScim** Scim Configuration.

Options

- **app-service**
  Specifies the name of the application service to which the object belongs. The default value is **none**. **Note:** If the **strict-updates** option is **enabled** on the application service that owns the object, you cannot modify or delete the object. Only the application service can modify or delete the object.
- **description**
  Specifies a unique description for the scim configuration. The default is **none**.
- **[name]**
  Specifies the name of the scim configuration. This option is required.
- **auth-server**
  Specifies LDAP Server which uses the scim configuration. The default is **none**.
- **group-dn**
  Specifies ‘group distinguished name’ attribute in directory to be used by scim configuration. The default is **none**.
- **group-obj-class**
  Specifies ‘group object class’ attribute in directory to be used by scim configuration. The default is **none**.
- **rdn-attr**
  Specifies ‘Relative Distinguished Name’ attribute in directory to be used by scim configuration. The default is **none**.
- **user-obj-class**
  Specifies ‘User Object Class’ attribute in directory to be used by scim configuration. The default is **none**.

33

apm ntlm

- Introducing the apm ntlm module
- Alphabetical list of components

Introducing the apm ntlm module

You can use the tmsh components that reside within the apm ntlm module to configure NTLM for the BIG-IP® Access Policy Manager®. For more information about the tmsh hierarchical structure, see Chapter 2, *Understanding and Using the Traffic Management Shell*.

Alphabetical list of components

The remainder of this chapter lists the tmsh components that are available in the apm ntlm module.

machine-account

Configures an APM NTLM machine account object.

Syntax

Configure the ntlm **machine account** using the syntax shown in the following sections.

Create/Modify

```
create machine-account [name]
    action [noop]
    administrator-name [[string] | none]
    administrator-password [[string] | none]
    app-service [[string] | none]
    domain-controller-fqdn [fqdn]
    domain-fqdn [fqdn]
    machine-account-name [[string] | none]
modify machine-account [name]
    action [change-password | noop]
    app-service [[string] | none]
    domain-controller-fqdn [fqdn]
    domain-fqdn [fqdn]
    machine-account-name [[string] | none]
edit machine-account [ [ [name] | [glob] | [regex] ] ... ]
    all-properties
    non-default-properties
```

Display

```
list machine-account
list machine-account [ [ [name] | [glob] | [regex] ] ... ]
```

Delete

```
delete machine-account [name]
```

Description

You can use the **machine-account** component to configure a NTLM machine account.

Examples

- **create machine-account myaccount {**
  machine-account-name "my_account_name"
  domain-fqdn "company.com"
  domain-controller-fqdn "server01.company.com"

```
    administrator-name "administrator"
    administrator-password "!My123Password"
}
```

Creates a NTLM machine account named **myaccount** in the **company.com** domain, with domain controller **server01.company.com**, administrator name **administrator** and administrator password **!My123Password**.

- **list machine-account**
  Displays a list of all NTLM machine accounts created on the system.
- **delete machine-account myaccount**
  Deletes the NTLM machine account named **myaccount** the system.

Options

- **machine-account-name**
  Specifies the name of the machine account.
- **domain-fqdn**
  Specifies the Fully Qualified Domain Name. This setting is required.
- **domain-controller**
  Specifies the Fully Qualified Domain Name (FQDN) of the domain controller for the domain specified in the **domain-fqdn** option. The default is **none**.
- **administrator-name**
  Specifies the name of a user that has administrative permissions on an Active Directory server. This setting is required only when a new machine account is being created.
- **administrator-password**
  Specifies the password associated with **administrator-name**. This setting is required only when a new machine account is being created.
- **action**
  Specifies the action type. To change the machine account password, type this action: change-password else no-op
- **app-service**
  Specifies the name of the application service to which the object belongs. The default value is **none**. **Note:** If the **strict-updates** option is **enabled** on the application service that owns the object, you cannot modify or delete the object. Only the application service can modify or delete the object.
  - **change-password**
    Specifies that you want to change the machine account password.
  - **no-op**
    Specifies "no operation performed". This is the default.

See Also

ntlm-auth

ntlm-auth

Configures an APM NTLM authentication object.

Syntax

Configure the **ntlm-auth** using the syntax shown in the following sections.

Create/Modify

```
create ntlm-auth [name]
    app-service [[string] | none]
    dc-fqdn-list [add | delete | modify | replace-all-with] {
        [[string]]
    }
    machine-account-name [[string] | none]
modify ntlm-auth [name]
    app-service [[string] | none]
    dc-fqdn-list [add | delete | modify | replace-all-with] {
        [[string]]
    }
    machine-account-name [[string] | none]
edit ntlm-auth [ [ [name] | [glob] | [regex] ] ... ]
    all-properties
    non-default-properties
```

Display

```
list ntlm-auth
list ntlm-auth [ [ [name] | [glob] | [regex] ] ... ]
```

Delete

```
delete ntlm-auth [name]
```

Description

You can use the **ntlm-auth** component to configure an NTLM authentication object.

Examples

- **create ntlm-auth myaccount {**
  dc-fqdn-list add {
  server01.company.com
  }
  machine-account-name "my_account"
  }

Creates a NTLM authentication object named **myaccount** with machine account **my_account**, and the list of domain controllers specified by **dc-fqdn-list**

- **list ntlm-auth**
  Displays a list of all NTLM authentication objects created on the system.
- **delete ntlm-auth myaccount**
  Deletes the NTLM authentication object named **myaccount** from the system.

Options

- **dc-fqdn-list**
  Specifies a list of Fully Qualified Domain Names (FQDNs) for the domain controllers to use for NTLM authentication.
- **machine-account-name**
  Specifies the NTLM machine account object name to use for this NTLM authentication
- **app-service**
  Specifies the name of the application service to which the object belongs. The default value is **none**. **Note:** If the **strict-updates** option is **enabled** on the application service that owns the object, you cannot modify or delete the object. Only the application service can modify or delete the object.

See Also

machine-account

34

apm policy

- Introducing the apm policy module
- Alphabetical list of components

Introducing the apm policy module

You can use the tmsh components that reside within the apm policy module to configure BIG-IP® Access Policy Manager®. For more information about the tmsh hierarchical structure, see Chapter 2, *Understanding and Using the Traffic Management Shell*.

Alphabetical list of components

The remainder of this chapter lists the tmsh components that are available in the apm policy module.

access-policy

Manages an access policy.

Syntax

WARNING

F5 Networks recommends that you use the visual policy editor in the Configuration utility to create and manage access policies.

customization-group

Manages a customization group.

Syntax

WARNING

F5 Networks recommends that you use the Configuration utility to create and manage customization groups.

See Also

apm policy agent, *apm profile*

image-file

Manages a file that contains an image.

Syntax

WARNING

F5 Networks recommends that you use the Configuration utility to create and manage image files.

See Also

apm policy agent, *apm profile*

policy-item

Manages an access policy item.

Syntax

WARNING

F5 Networks recommends that you use the visual policy editor in the Configuration utility to create and manage access policy items.

Warning: This page is obsolete. Windows Group Policy is no longer supported.
windows-group-policy-file - Manages FullArmor GPAnywhere Windows group policy files.

Syntax

WARNING

F5 Networks recommends that you use the visual policy editor in the Configuration utility to create and manage FullArmor GPAnywhere Windows group policy files.

35

apm policy agent

- Introducing the apm policy agent module
- Alphabetical list of components

Introducing the apm policy agent module

You can use the tmsh components that reside within the apm policy agent module to configure BIG-IP® Access Policy Manager®. For more information about the tmsh hierarchical structure, see Chapter 2, *Understanding and Using the Traffic Management Shell*.

Alphabetical list of components

The remainder of this chapter lists the tmsh components that are available in the apm policy agent module.

aaa-active-directory

Manages an AAA Active Directory® agent.

Syntax

Configure the **aaa-active-directory** component within the **policy agent** module using the following syntax.

Create/Modify

```
create aaa-active-directory [name]
modify aaa-active-directory [name]
  options
    app-service [[string] | none]
    auth-max-logon-attempt [integer]
    fetch-nested-groups [true | false]
    fetch-primary-groups [true | false]
    hints [true | false]
    query-attrname [[string] | none]
    query-filter [[string] | none]
    server [[string] | none]
    trusted-domains [[string | none]]
    show-extended-error [true | false]
    type [query | auth | last]
    upn [true | false]
```

Display

```
list aaa-ldap
list aaa-ldap [ [ [name] | [glob] | [regex] ] ... ]
show running-config aaa-ldap
show running-config aaa-ldap [ [ [name] | [glob] | [regex] ] ... ]
    all
    all-properties
    current-module
    non-default-properties
    one-line
    app-service
    partition
```

Delete

```
delete aaa-active-directory ([name] | all)
```

Description

You can use the **aaa-active-directory** component to configure an AAA Active Directory agent.

Examples

- **create aaa-active-directory MyADQueryagent**
  {query-filter "(be
  sAMAccountName=%{session.logon.last.username})"
  type query
  server "companyAD"
  }
  Creates the **query** type AAA Active Directory agent named **MyADQueryagent** that uses the **(be sAMAccountName=%{session.logon.last.username})** filter and the **companyAD** AAA AD Server.
- **create agent aaa active MyADAuthagent {**
  type auth
  server "companyAD"
  }
  Creates the **authorization** type AAA Active Directory agent named **MyADAuthagent** that uses the **companyAD** AAA AD server.
- **list aaa-active-directory all**
  Displays a list of AAA Active Directory agents and their properties.
- **delete aaa-active-directory MyADagent**
  Deletes the **MyADagent** AAA Active Directory agent.

Options

- **app-service**
  Specifies the name of the application service to which the object belongs. The default value is **none**. **Note:** If the **strict-updates** option is **enabled** on the application service that owns the object, you cannot modify or delete the object. Only the application service can modify or delete the object.
- **auth-max-logon-attempt**
  Specifies the maximum number of opportunities that users have to re-enter credentials after their first attempt to log in fails. If you set this value to a number from **2** to **5** inclusive, the system allows users the specified number of opportunities to log in after the first attempt to log in fails. If you set the value to **1**, the system does not allow a second log in opportunity after a first log in attempt fails. The default value is **3**.
- **fetch-nested-groups**
  When enabled, the system administrator can retrieve the full list of groups that user belongs to, even if the retrieval privileges are nested through other groups to which the user belongs to directly. The default value is **false**.
- **fetch-primary-groups**
  When enabled, the system administrator can retrieve the primary group of a user, and use that name as a group in access policy item rules. The default value is **false**.

- **hints**
  When enabled, the system offers the user an option to create a hint that assists in remembering a password. The default value is **false**.
- **query-attrname**
  Specifies the attribute name that you are adding or deleting for the agent.
- **query-filter**
  Specifies the search criteria the system uses when querying an AAA Active Directory® server for authentication information. The system supports session variables as part of search query string.
- **[name]**
  Specifies the name of an AAA Active Directory agent. This setting is required.
- **partition**
  Displays the partition within which the component resides.
- **server**
  Specifies an AAA Active Directory server the system uses for Active Directory queries and authentication.
- **server**
  Specifies an AAA Active Directory Trusted Domains object that the system uses for Active Directory queries and authentication. This option requires **upn** option to be enabled
- **show-extended-error**
  Specifies to display a verbose error message. The default value is **false**.
- **type**
  Specifies the type of AAA Active Directory agent. The default value is **last**.
  - **query**
    Specifies that the agent makes a query against the AAA Active Directory Server to retrieve information in accordance with the **query-filter** and **query-attributes** options.
  - **auth**
    Specifies that the agent is an authentication agent only. It uses the AAA Active Directory Server, but only for authentication purposes. APM does not get any information from the Domain.
  - **last**
- **upn**
  When enabled, APM supports the user principal name (UPN) naming style and process cross-domain authentication requests. Some examples of UPNs are: **user@fqdn.of.domain.com**, **user@upnsuffix.com**, and **user@domain**. The default value is **false**.

See Also

tmsh

aaa-client-cert

Manages an AAA Client Certification agent.

Syntax

Configure the **aaa-client-cert** component within the **policy-agent** module using the following syntax.

Create/Modify

```
modify aaa-client-cert [name]
create aaa-client-cert [name]
    app-service [[string] | none]
    mode [request | require]
```

Display

```
list aaa-client-cert
list aaa-client-cert [ [ [name] | [glob] | [regex] ] ... ]
show running-config aaa-client-cert
show running-config aaa-client-cert [ [ [name] | [glob] | [regex] ] ... ]
    all
    all-properties
    current-module
    non-default-properties
    one-line
    app-service
    partition
```

Delete

```
delete aaa-client-cert [name]
```

Description

You can use this component to configure an AAA Client Certification agent.

Examples

- **create aaa-client-cert MyCCagent**
  Creates the AAA Client Certification agent named **MyCCagent** in the Common partition.
- **list aaa-client-cert all**
  Displays a list of AAA Client Certification agents.
- **delete aaa-client-cert MyCCagent**
  Deletes the **MyCCagent** AAA Client Certification agent.

Options

- **[name]**
  Specifies the name of an AAA client cert agent. This setting is required.
- **app-service**
  Specifies the name of the application service to which the object belongs. The default value is **none**. **Note:** If the **strict-updates** option is **enabled** on the application service that owns the object, you cannot modify or delete the object. Only the application service can modify or delete the object.
- **mode**
  Specifies the mode (request/require) for this certificate. The options are:
  - **request**
    Specifies that the system requests a valid certificate from a client, but always authenticates the client.
  - **require**
    Specifies that the system requires a client to present a valid certificate.
- **partition**
  Displays the partition within which the component resides.

See Also

tmsh

aaa-crldp

Manages an AAA CRLDP (Constraint-Based Routed Label Distributed Protocol) agent.

Syntax

Configure the **aaa-crldp** component within the **policy agent** module using the following syntax.

Create/Modify

```
create aaa-crldp [name]
modify aaa-crldp [name]
    app-service [[string] | none]
    server (<string> | none)
```

Display

```
list aaa-crldp
list aaa-crldp [ [ [name] | [glob] | [regex] ] ... ]
show running-config aaa-crldp
show running-config aaa-crldp [ [ [name] | [glob] | [regex] ] ... ]
    all
    all-properties
    app-service
    current-module
    non-default-properties
    one-line
    partition
```

Delete

```
delete aaa-crldp [name]
```

Description

You can use the **aaa-crldp** component to create and manage an AAA CRLDP agent.

Examples

- **create aaa-crldp MyCCagent**
  Creates an AAA CRLDP agent named **MyCCagent** in the Common partition.
- **list aaa-crldp all**
  Displays a list of AAA CRLDP agents.
- **delete aaa-crldp MyCCagent**
  Deletes the **MyCCagent** AAA CRLDP agent.

Options

- **[name]**
  Specifies the name of an agent that you want to display or delete. This setting is required.
- **partition**
  Displays the partition within which the component resides.
- **app-service**
  Specifies the name of the application service to which the object belongs. The default value is **none**. **Note:** If the **strict-updates** option is **enabled** on the application service that owns the object, you cannot modify or delete the object. Only the application service can modify or delete the object.
- **server**
  Specifies the name of the server on which this agent resides. This option is required.

See Also

tmsh

aaa-http

Manages an AAA HTTP agent.

Syntax

Configure the **aaa-http** component within the **policy agent** module using the following syntax.

Create/Modify

```
create aaa-http [name]
modify aaa-http [name]
  options
    app-service [[string] | none]
    max-logon-attempt [integer]
    server [[string] | none]
```

Display

```
list aaa-http
list aaa-http [ [ [name] | [glob] | [regex] ] ... ]
show running-config aaa-http
show running-config aaa-http [ [ [name] | [glob] | [regex] ] ... ]
    all
    all-properties
    current-module
    non-default-properties
    one-line
    app-service
    partition
```

Delete

```
delete aaa-http [name]
```

Description

You can use the **aaa-http** component to configure an AAA HTTP agent.

Examples

- **create aaa-http MyCCagent**
  Creates the aaa-http agent named **MyCCagent** in the Common partition.
- **list all aaa-http**
  Displays a list of aaa-http agents.
- **delete aaa-http MyCCagent**
  Deletes the **MyCCagent** aaa-http agent.

Options

- **app-service**
  Specifies the name of the application service to which the object belongs. The default value is **none**. **Note:** If the **strict-updates** option is **enabled** on the application service that owns the object, you cannot modify or delete the object. Only the application service can modify or delete the object.
- **max-logon-attempt**
  Specifies the maximum number of opportunities that users have to re-enter credentials after their first attempt to log in fails. If you set this value to a number from **2** to **5** inclusive, the system allows users the specified number of opportunities to log in after the first attempt to log in fails. If you set the value to **1**, the system does not allow a second log in opportunity after a first log in attempt fails. The default value is **3**.
- **[name]**
  Specifies the name of an AAA HTTP agent. This setting is required.
- **partition**
  Displays the partition within which the component resides.
- **server**
  Specifies which AAA HTTP server the system uses for Active Directory queries and authentication.

See Also

tmsh

aaa-ldap

Manages an AAA LDAP® agent.

Syntax

Configure the **aaa-ldap** component within the **policy agent** module using the following syntax.

Create/Modify

```
create aaa-ldap [name]
modify aaa-ldap [name]
    app-service [[string] | none]
    attr-name (<string list> | none) [add | delete]
    filter [[string] | none]
    group-member-scope [none | direct | all]
    group-membership-scope [none | direct | all]
    max-logon-attempt [integer]
    search-dn [[string] | none]
    server [[string] | none]
    show-extended-error [true | false]
    type [query | auth | modify | last]
    user-dn [[string] | none]
    modify-type [add | modify | delete | modify-last]
    ldapmod-attributes (<ldapmod attribute list> | none) [add | delete]
```

Display

```
list aaa-ldap
list aaa-ldap [ [ [name] | [glob] | [regex] ] ... ]
show running-config aaa-ldap
show running-config aaa-ldap [ [ [name] | [glob] | [regex] ] ... ]
    all
    all-properties
    current-module
    non-default-properties
    one-line
    app-service
    partition
```

Delete

```
delete aaa-ldap [name]
```

Description

Use this component to create, modify, display, or delete an AAA LDAP agent.

Examples

- **create aaa-ldap MyLDAPagent {**
  user-dn
  "cn=%{session.logon.last.username},cn=users,dc=lab,dc=fp,dc=com
  "
  type auth
  server "companyLDAP"
  }
  aaa-ldap MyLDAPagent {
  search-dn "cn=users,dc=lab,dc=fp,dc=com"
  filter "(SAMAccountName=%{{session.logon.last.username}})"
  type auth
  server "companyLDAP"
  }

  Creates the authorization type AAA LDAP agent named **MyLDAPagent** that is associated with the **companyLDAP** server that uses the **cn=%{session.logon.last.username},cn=users,dc=lab,dc=fp,dc=f5net, dc=com** user domain name, the **cn=users,dc=lab,dc=fp,dc=com** search domain, and the **(SAMAccountName=%{{session.logon.last.username}})** filter.
- **create aaa-ldap MyLDAPagent {**
  search-dn "cn=users,dc=lab,dc=fp,dc=com"
  filter "(sAMAccountName=%{{session.logon.last.username}})"
  type query
  server "companyLDAP"
  }

  Creates the **query** type AAA LDAP agent named **MyLDAPagent** that is associated with the **companyLDAP** server that uses the **cn=users,dc=lab,dc=fp,dc=com** search domain and the **(SAMAccountName=%{{session.logon.last.username}})** filter.
- **create aaa-ldap MyLDAPagent {**
  user-dn
  "cn=%{session.logon.last.username},cn=users,dc=lab,dc=fp,dc=com
  "
  type modify
  modify-type add
  server "companyLDAP"
  ldapmod-attributes add { objectClass { mod-op add mod-values add { top person organizationalPerson user } } cn { mod-op add mod-values add { demo } } }
  }

  Creates the modify type AAA LDAP agent named **MyLDAPagent** that is associated with the **companyLDAP** server that uses the **cn=%{session.logon.last.username},cn=users,dc=lab,dc=fp,dc=f5net, dc=com** user domain name, the **add** modify type, and the ldapmod attributes
- **create aaa-ldap MyLDAPagent {**
  user-dn
  "cn=%{session.logon.last.username},cn=users,dc=lab,dc=fp,dc=com
  "

type modify
modify-type modify
server "companyLDAP"
ldapmod-attributes add { givenName { mod-op replace mod-values add { demo } } }
}

Creates the modify type AAA LDAP agent named **MyLDAPagent** that is associated with the **companyLDAP** server that uses the **cn=%{session.logon.last.username},cn=users,dc=lab,dc=fp,dc=f5net,dc=com** user domain name, the **modify** modify type, and the ldapmod attributes which uses **givenName** modify attribute **replace** mod operation and the **demo** mod values

- **create aaa-ldap MyLDAPagent {**
  user-dn "cn=%{session.logon.last.username},cn=users,dc=lab,dc=fp,dc=com"
  type modify
  modify-type delete
  server "companyLDAP"
  }

  Creates the modify type AAA LDAP agent named **MyLDAPagent** that is associated with the **companyLDAP** server that uses the **cn=%{session.logon.last.username},cn=users,dc=lab,dc=fp,dc=f5net,dc=com** user domain name, the **delete** modify type
- **list aaa-ldap**
  Displays a list of AAA LDAP agents.
- **delete aaa-ldap MyLDAPagent**
  Deletes the **MyLDAPagent** AAA LDAP agent.

Options

- **app-service**
  Specifies the name of the application service to which the object belongs. The default value is **none**. **Note:** If the **strict-updates** option is **enabled** on the application service that owns the object, you cannot modify or delete the object. Only the application service can modify or delete the object.
- **attr-name**
  Adds an attribute name to the agent or deletes an attribute name from the agent.
- **group-member-scope**
  Specifies the scope of user lookup for a group. When the search returns a group, this attribute specifies whether to also look up the members of the group. The options are:
  - **none**No members required.
  - **direct**Only direct members required.

- **all**All members required. This includes those that derive membership in this group through membership in other groups and those that are direct members.

- **group-membership-scope**
  Specifies the scope of group lookup for a user or a group. When the search returns a user or a group, this attribute specifies whether to also look up the groups to which this user or group belong. The options are:
  - **none**No groups required.
  - **direct**Only the groups to which the current user or group belong directly are required.
  - **all**All groups required. This includes the groups to which the user or the group belong directly and the groups to which the user or group belong indirectly (through membership in another group).

- **filter**
  Specifies the LDAP filter that APM uses when querying an AAA LDAP server for authentication information. You must use the filter option with the **search-dn** option.
- **max-logon-attempt**
  Specifies the maximum number of opportunities that users have to re-enter credentials after their first attempt to log in fails. If you set this value to a number from **2** to **5** inclusive, the system allows users the specified number of opportunities to log in after the first attempt to log in fails. If you set the value to **1**, the system does not allow a second log in opportunity after a first log in attempt fails. The default value is **3**.
- **[name]**
  Specifies the name of an AAA LDAP agent. This setting is required.
- **partition**
  Displays the partition within which the component resides.
- **search-dn**
  Specifies the base domain name that APM uses for internal LDAP search operations. You must use the **search-dn** option with the **filter** option.
- **server**
  Specifies the AAA LDAP server that the system uses for LDAP queries and authentication.
- **show-extended-error**
  Specifies to display a verbose error message. The default value is **false**.
- **type**
  Specifies a type of AAA LDAP agent. This setting is required. The default is **last**.

- **user-dn**
  Specifies the fully qualified domain name of the Access Policy Manager. F5 Networks recommends that you specify this value in lower case and without spaces for compatibility with some specific LDAP servers. The specific content of this string depends on your directory layout.

See Also

tmsh

aaa-ocsp

Manages an AAA OCSP (Online Certificate Status Protocol) agent.

Syntax

Configure the **aaa-ocsp** component within the **policy agent** module using the following syntax.

Create/Modify

```
create aaa-ocsp [name]
modify aaa-ocsp [name]
    app-service [[string] | none]
    ocsp-responder <string>
```

Display

```
list aaa-ocsp
list aaa-ocsp [ [ [name] | [glob] | [regex] ] ... ]
show running-config aaa-ocsp
show running-config aaa-ocsp [ [ [name] | [glob] | [regex] ] ... ]
    all
    all-properties
    current-module
    non-default-properties
    one-line
    app-service
    partition
```

Delete

```
delete aaa-ocsp [name]
```

Description

Use this command to create, modify, display, or delete an AAA OCSP agent.

Examples

- **create aaa-ocsp MyCCagent**
  Creates the AAA OCSP agent named **MyCCagent** in the Common partition.
- **list aaa-ocsp all**
  Displays a list of AAA OCSP agents.
- **delete aaa-ocsp MyCCagent**
  Deletes the **MyCCagent** AAA OCSP agent.

Options

- **[name]**
  Specifies the name of an agent that you want to display or delete. This setting is required.
- **app-service**
  Specifies the name of the application service to which the object belongs. The default value is **none**. **Note:** If the **strict-updates** option is **enabled** on the application service that owns the object, you cannot modify or delete the object. Only the application service can modify or delete the object.
- **ocsp-responder**
- **partition**
  Displays the partition within which the object resides.

aaa-radius

Manages an AAA RADIUS agent.

Syntax

Configure the **aaa-radius** component within the **policy agent** module using the following syntax.

Create/Modify

```
create aaa-radius [name]
modify aaa-radius [name]
     app-service [[string] | none]
     max-logon-attempt <number>
     server (<string> | none)
     show-extended-error (true | false)
```

Display

```
list aaa-radius
list aaa-radius [ [ [name] | [glob] | [regex] ] ... ]
show running-config aaa-radius
show running-config aaa-radius [ [ [name] | [glob] | [regex] ] ... ]
    all
    all-properties
    current-module
    non-default-properties
    one-line
    app-service
    partition
```

Delete

```
delete aaa-radius [name]
```

Description

Use this command to create, modify, display, or delete an AAA RADIUS agent.

Examples

- **create aaa-radius Myradiusagent {server "companyradius"}**
  Creates an AAA RADIUS agent named **Myradiusagent** that is associated with the **companyradius** server.
- **list aaa-radius**
  Displays a list of AAA RADIUS agents.

- **delete aaa-radius Myradiusagent**
  Deletes the **Myradiusagent** AAA RADIUS agent.

Options

- **app-service**
  Specifies the name of the application service to which the object belongs. The default value is **none**. **Note:** If the **strict-updates** option is **enabled** on the application service that owns the object, you cannot modify or delete the object. Only the application service can modify or delete the object.
- **max-logon-attempt**
  Specifies the maximum number of opportunities that users have to re-enter credentials after their first attempt to log in fails. If you set this value to a number from **2** to **5** inclusive, the system allows users the specified number of opportunities to log in after the first attempt to log in fails. If you set the value to **1**, the system does not allow a second log in opportunity after a first log in attempt fails. The default value is **3**.
- **[name]**
  Specifies the name of an aaa radius agent. This setting is required.
- **partition**
  Displays the partition within which the object resides.
- **server**
  Specifies the AAA RADIUS server that the system uses for RADIUS queries and authentication.
- **show-extended-error**
  Specifies to display a verbose error message. The default value is **false**.

See Also

tmsh

aaa-securid

Manages an AAA SecurID agent.

Syntax

Configure the **aaa-securid** component within the **policy agent** module using the following syntax.

Create/Modify

```
create aaa-securid [name]
modify aaa-securid [name]
    app-service [[string] | none]
    max-logon-attempt [integer]
    server [[string] | none]
    show-extended-error [true | false]
edit aaa-securid | [glob] | [regex] ] ... ]
    all-properties
    non-default-properties
```

Display

```
list aaa-securid
list aaa-securid [ [ [name] | [glob] | [regex] ] ... ]
show running-config aaa-securid
show running-config aaa-securid [ [ [name] | [glob] | [regex] ] ... ]
    all
    all-properties
    current-module
    non-default-properties
    one-line
    app-service
    partition
```

Delete

```
delete aaa-securid [name]
```

Description

You can use the **aaa-securid** component to create and manage an AAA SecurID agent.

Examples

- **create aaa-securid mySecuridAgent { server rsa1_106 }**
  Creates an AAA SecurID agent named **mySecuridAgent** that is associated to AAA RSA Server **rsa1_106**.

- **list all aaa-securid**
  Displays a list of AAA SecurID agents.
- **delete aaa-securid MyCCagent**
  Deletes the **MyCCagent** AAA Client Certification agent.

Options

- **[name]**
  Specifies the name of an agent that you want to display or delete. This setting is required.
- **partition**
  Displays the partition within which the component resides.
- **app-service**
  Specifies the name of the application service to which the object belongs. The default value is **none**. **Note:** If the **strict-updates** option is **enabled** on the application service that owns the object, you cannot modify or delete the object. Only the application service can modify or delete the object.
- **max-logon-attempt**
  Specifies the maximum number of opportunities that users have to re-enter credentials after their first attempt to log in fails. If you set this value to a number from **2** to **5** inclusive, the system allows users the specified number of opportunities to log in after the first attempt to log in fails. If you set the value to **1**, the system does not allow a second log in opportunity after a first log in attempt fails. The default value is **3**.
- **server**
  Specifies the AAA RSA SecurID server that the system uses for LDAP queries and authentication.
- **show-extended-error**
  Specifies to display a verbose error message. The default value is **false**.

See Also

tmsh

acct-radius

Manages a RADIUS Account agent.

Syntax

Configure the **acct-radius** component within the **policy agent** module using the following syntax.

Create/Modify

```
create acct-radius [name]
modify acct-radius [name]
     app-service [[string] | none]
     server [[string] | none]
edit acct-radius | [glob] | [regex] ] ... ]
    all-properties
    non-default-properties
```

Display

```
list acct-radius
list acct-radius [ [ [name] | [glob] | [regex] ] ... ]
show running-config acct-radius
show running-config acct-radius [ [ [name] | [glob] | [regex] ] ... ]
    all
    all-properties
    current-module
    non-default-properties
    one-line
    app-service
    partition
```

Delete

```
delete acct-radius [name]
```

Description

You can use the **acct-radius** component to create and manage an RADIUS Account agent.

Examples

- **create acct-radius MyRADIUSagent {**
  server "MyRADIUS"
  }

  Creates the **MyRADIUSagent** RADIUS Account agent that is associated with the **MyRADIUS** server.

- **list acct-radius**
  Displays a list of RADIUS Account agents and the servers associated with the agents.
- **delete acct-radius MyRADIUSagent**
  Deletes the **MyRADIUSagent** RADIUS Account agent.

Options

- **[name]**
  Specifies the name of an RADIUS Account server. This setting is required.
- **partition**
  Displays the partition within which the component resides.
- **app-service**
  Specifies the name of the application service to which the object belongs. The default value is **none**. **Note:** If the **strict-updates** option is **enabled** on the application service that owns the object, you cannot modify or delete the object. Only the application service can modify or delete the object.
- **server**
  Specifies an RADIUS Account server the system uses for RADIUS queries and authentication. This option is required.

See Also

tmsh

acct-tacacsplus

Manages a TACACS+® Account agent.

Syntax

Configure the **acct-tacacsplus** component within the **policy agent** module using the following syntax.

Create/Modify

```
create acct-tacacsplus [name]
modify acct-tacacsplus [name]
  options
    app-service [[string] | none]
    server [[string] | none]
```

Display

```
list acct-tacacsplus
list acct-tacacsplus [ [ [name] | [glob] | [regex] ] ... ]
show running-config acct-tacacsplus
show running-config acct-tacacsplus  [ [ [name] | [glob] | [regex] ] ... ]
    all
    all-properties
    current-module
    non-default-properties
    app-service
    partition
```

Delete

```
delete acct-tacacsplus [name]
```

Description

You can use the **acct-tacacsplus** component to configure a TACACS+ Account agent.

Examples

- **create acct-tacacsplus MyADQueryagent {**
  server "companyAD"
  }
  Creates the agent type TACACS+ Account named **MyADQueryagent** that uses the **companyAD** server.
- **list acct-tacacsplus all**
  Displays a list of TACACS+ Account agents and the server associated with each agent.

- **delete acct-tacacsplus MyADagent**
  Deletes the **MyADagent** TACACS+ Account agent.

Options

- **[name]**
  Specifies the name of an acct-tacacsplus agent. This setting is required.
- **partition**
  Displays the partition within which the component resides.
- **app-service**
  Specifies the name of the application service to which the object belongs. The default value is **none**. **Note:** If the **strict-updates** option is **enabled** on the application service that owns the object, you cannot modify or delete the object. Only the application service can modify or delete the object.
- **server**
  Specifies the TACACS+ Account server that the system uses for queries and authentication.

See Also

tmsh

decision-box

Manages a Decision Box agent.

Syntax

Configure the **decision-box** component within the **policy agent** module using the following syntax.

Create/Modify

```
create decision-box [name]
modify decision-box [name]
  options
    app-service [[string] | none]
    customization-group [name]
```

Display

```
list decision-box
list decision-box [ [ [name] | [glob] | [regex] ] ... ]
show running-config decision-box
show running-config decision-box  [ [ [name] | [glob] | [regex] ] ... ]
    all
    all-properties
    app-service
    current-module
    non-default-properties
    one-line
    partition
```

Delete

```
delete decision-box ([name] | all)
```

Description

You can use the **decision-box** component to configure a Decision Box agent.

Examples

- **create dynamic-acl MyADQueryagent**
  Creates the Decision Box agent named **MyADQueryagent**.
- **list decision-box all**
  Displays a list of Decision Box agents.
- **delete decision-box MyADagent**
  Deletes the **MyADagent** Decision Box agent.

Options

- **app-service**
  Specifies the name of the application service to which the object belongs. The default value is **none**. **Note:** If the **strict-updates** option is **enabled** on the application service that owns the object, you cannot modify or delete the object. Only the application service can modify or delete the object.
- **customization-group**
  Specifies the name of the existing customization group to which the agent belongs.
- **[name]**
  Specifies the name of a Decision Box agent. This setting is required.
- **partition**
  Displays the partition within which the component resides.

See Also

tmsh

dynamic-acl

Manages a Dynamic ACL agent.

Syntax

Configure the **dynamic-acl** component within the **policy agent** module using the following syntax.

Create/Modify

```
create dynamic-acl [name]
modify dynamic-acl [name]
  options
    app-service [[string] | none]
    entries [ add | delete | modify | none | replace-all-with]
```

Display

```
list dynamic-acl
list dynamic-acl [ [ [name] | [glob] | [regex] ] ... ]
show running-config dynamic-acl
show running-config dynamic-acl  [ [ [name] | [glob] | [regex] ] ... ]
    all
    all-properties
    app-service
    current-module
    non-default-properties
    one-line
    partition
```

Delete

```
delete dynamic-acl [name]
```

Description

You can use the **dynamic-acl** component to create and manage a Dynamic access control list (acl) agent that parses ACL text input with a specified format from a specified session variable, assigns the parsed entry into a Dynamic ACL object, and assigns it into a current user session. An ACL is a set of restrictions associated with a resource or favorite that defines access for users and groups.

Examples

- **create dynamic-acl <dynamic-acl-agent-name** { entries <operator> { <index> { acl <DynamicACLentry> [format [f5 | cisco]] source <session.variable source> } } }>
  Creates the Dynamic ACL agent named **MyDynamicAclAgent**.

- **list dynamic-acl**
  Displays a list of Dynamic ACL agents.
- **delete dynamic-acl MyDynamicAclAgent**
  Deletes the Dynamic ACL agent named **MyDynamicAclAgent**.

Options

- **app-service**
  Specifies the name of the application service to which the object belongs. The default value is **none**. **Note:** If the **strict-updates** option is **enabled** on the application service that owns the object, you cannot modify or delete the object. Only the application service can modify or delete the object.
- **entries**
  Specifies the name of the entry to assign this dynamic access control list.
- **[name]**
  Specifies the name of the Dynamic Acl agent. This setting is required.
- **partition**
  Displays the partition within which the component resides.

See Also

tmsh

ending-allow

Manages an Ending Allow agent.

Syntax

Configure the **ending-allow** component within the **policy agent** module using the following syntax.

Create/Modify

```
create ending-allow [name]
modify ending-allow [name]
    app-service [[string] | none]
```

Display

```
list ending-allow
list ending-allow [ [ [name] | [glob] | [regex] ] ... ]
show running-config ending-allow
show running-config ending-allow  [ [ [name] | [glob] | [regex] ] ... ]
    all
    all-properties
    app-service
    current-module
    non-default-properties
    one-line
    partition
```

Delete

```
delete ending-allow ([name] | all)
```

Description

Access policy endings indicate the final outcome of a branch of an access policy. An Allow ending is a successful ending in which the system displays the user's home page and grants access to a webtop connection.

Examples

- **create ending-allow MyEndingAllowAgent { }**
  Creates the Ending Allow agent named **MyEndingAllowAgent**.
- **list ending-allow**
  Displays a list of Ending Allow agents.
- **delete ending-allow MyEndingAllowAgent**
  Deletes the Ending Allow agent named **MyEndingDeniedAgent**.

Options

- **[name]**
  Specifies the name of an Ending Allow agent. This option is required.
- **app-service**
  Specifies the name of the application service to which the object belongs. The default value is **none**. **Note:** If the **strict-updates** option is **enabled** on the application service that owns the object, you cannot modify or delete the object. Only the application service can modify or delete the object.
- **partition**
  Displays the partition within which the component resides.

See Also

tmsh

ending-deny

Manages an Ending Deny agent.

Syntax

Configure the **ending-deny** component within the **policy agent** module using the following syntax.

Create/Modify

```
create ending-deny [name]
modify ending-deny [name]
  options
    app-service [[string] | none]
    customization-group [name]
```

Display

```
list ending-deny
list ending-deny [ [ [name] | [glob] | [regex] ] ... ]
show running-config ending-deny
show running-config ending-deny  [ [ [name] | [glob] | [regex] ] ... ]
    all
    all-properties
    app-service
    current-module
    non-default-properties
    one-line
    partition
```

Delete

```
delete ending-deny ([name] | all)
```

Description

Access policy endings indicate the final outcome of a branch of an access policy. The Logon Deny ending is the final result of an unsuccessful logon attempt (the failure could be caused by an incorrect logon attempt, a security requirement incompatibility, or the use of an unsupported device). Upon reaching a Logon Deny ending, the user sees an error message. You can use the **ending-deny** component to create and manage an Ending Deny agent.

Examples

- **create ending-deny MyEndingDenyAgent customization-group MyLogOffCG**
  Creates the Ending Deny agent named **MyEndingDenyAgent** that is associated with the **MyLogOffCG** customization group.

- **list ending-deny**
  Displays a list of Ending Deny agents.
- **delete ending-deny MyEndingDenyAgent**
  Deletes the Ending Deny agent named **MyEndingDenyAgent**.

Options

- **app-service**
  Specifies the name of the application service to which the object belongs. The default value is **none**. **Note:** If the **strict-updates** option is **enabled** on the application service that owns the object, you cannot modify or delete the object. Only the application service can modify or delete the object.
- **customization-group**
  Specifies the name of the existing **customization-group** to which the agent belongs. It enables you to customizes the logon deny page. For example, you can indicate a specific reason for the denial of access. This setting is required, and the customization group that you assign must be of the type **logout**.
- **[name]**
  Specifies the name of an Ending Deny agent. This setting is required.
- **partition**
  Displays the partition within which the component resides.

See Also

tmsh

ending-redirect

Manages an Ending Redirect agent.

Syntax

Configure the **ending-redirect** component within the **policy agent** module using the following syntax.

Create/Modify

```
create ending-redirect [name]
modify ending-redirect [name]
  options
    app-service [[string] | none]
    close-session [true | false]
    url [value]
```

Display

```
list ending-redirect
list ending-redirect [ [ [name] | [glob] | [regex] ] ... ]
show running-config ending-redirect
show running-config ending-redirect  [ [ [name] | [glob] | [regex] ] ... ]
    all
    all-properties
    app-service
    current-module
    non-default-properties
    one-line
    partition
```

Delete

```
delete ending-redirect ([name] | all)
```

Description

The Redirect ending can be used to redirect the user, rather than allowing or denying a connection. It can also send a user directly to an update script or to different server or landing URI. Upon reaching a Redirect ending, the user sees a screen indicating that they are being redirected to a different URL. You can use the **ending-redirect** component to create and manage an Ending Redirect agent.

Examples

- **create ending-redirect MyEndingRedirectAgent { url "http://www.myweb.com" }**
  Creates the Ending Redirect agent named **MyEndingRedirectAgent** that

redirects a connection to http://www.myweb.com.
Creates an agent using the current protocol and the session variable **%{sesession.server.network.protocol}**

- **list ending-redirect**
  Displays a list of Ending Redirect agents.
- **delete ending-redirect MyEndingRedirectAgent**
  Deletes the Ending Redirect agent named **MyEndingRedirectAgent**.

Options

- **app-service**
  Specifies the name of the application service to which the object belongs. The default value is **none**. **Note:** If the **strict-updates** option is **enabled** on the application service that owns the object, you cannot modify or delete the object. Only the application service can modify or delete the object.
- **close-session**
  Redirects to the specified URI after closing the session if **enabled**. Otherwise, redirect to the specified URI without closing the session. The default is **enabled**.
- **[name]**
  Specifies the name of an Ending Redirect agent. This option is required.
- **url**
  Specifies the URL to which the system redirects the original request. This option is required, and you must specify an absolute URL.
  An absolute URL specifies the exact location of a file or directory on the Internet.

See Also

tmsh

endpoint-check-machine-cert

Manages an End-point Check Machine certificate agent.

Syntax

Configure the **endpoint-check-machine-cert** component within the **apm policy agent** module using the following syntax.

Create/Modify

```
create endpoint-check-machine-cert [name]
modify endpoint-check-machine-cert [name]
    app-service [[string] | none]
    ca-profile-name [value]
    issuer [value]
    match-rule  [any | issuer | issuer-and-serial-num | last  |
subject-alt-name-match-fqdn | subject-on-match-fqdn ]
    ocsp-responder-name [value]
    save-cert [ true| false]
    allow-elevation [ true| false]
    serial-number [integer]
    store-location [machine | user]
    store-name [value]
    subject-alt-name [value]
edit endpoint-check-machine-cert [ [ [name] | [glob] | [regex] ] ... ]
    all-properties
    non-default-properties
```

Display

```
list endpoint-check-machine-cert
list endpoint-check-machine-cert [ [ [name] | [glob] | [regex] ] ... ]
show running-config endpoint-check-machine-cert
show running-config endpoint-check-machine-cert  [ [ [name] | [glob] | [regex] ] ... ]
    all
    all-properties
    app-service
    current-module
    non-default-properties
    one-line
    partition
```

Delete

```
delete endpoint-check-machine-cert [name]
```

Description

Endpoint security is a centrally-managed method of monitoring and maintaining client-system security.

The **endpoint-check-machine-cert** component checks for the presence of a valid machine certificate on Windows/Mac client systems during access policy validation.

Examples

- **create endpoint-check-machine-cert MyMCagent**
  Creates the Endpoint Check Machine certificate agent named MyMCagent in the
  Common partition.
- B <list endpoint-check-machine-cert>
  Displays a list of Endpoint Check Machine certificate agents.
- **delete endpoint-check-machine-cert MyMCagent**
  Deletes the **MyMCagent** Endpoint Check Machine certificate agent.

Options

- **app-service**
  Specifies the name of the application service to which the object belongs. The default value is **none**. **Note:** If the **strict-updates** option is **enabled** on the application service that owns the object, you cannot modify or delete the object. Only the application service can modify or delete the object.
- **ca-profile-name**
  Specifies the name of the certificate authority profile to validate the certificate.
- **issuer**
  Specifies the name used to match the issuer name in the machine certificate.
- **match-rule**
  Specifies the match rule to look up the machine certificate on the client machine.
- **[name]**
  Specifies the name of an external logon page agent. This option is required.
- **ocsp-responder-name**
  Specifies the name of the OCSP responder to validate the certificate using OCSP.
- **partition**
  Displays the partition within which the component resides.
- **save-cert**
  Specifies to store the entire machine certificate in a session variable.
- **allow-elevation**
  Specifies to allow UAC prompts during private key checking.

- **serial-number**
  Specifies the serial number used to match the serial number of the machine certificate.
- **store-location**
  Specifies the location of the certificate store on the client machine.
- **store-name**
  Specifies the name of the certificate store on the client machine.
- **subject-alt-name**
  Specifies the name used to match the subject-alt-name in the machine certificate.
- **partition**
  Specifies the partition within which the object resides.

See Also

endpoint-check-software, *endpoint-linux-check-file*, *endpoint-linux-check-process*, *endpoint-mac-check-file*, *endpoint-mac-check-process*, *endpoint-windows-check-file*, *endpoint-windows-browser-cache-cleaner*, *endpoint-windows-check-process*, *endpoint-windows-check-registry*, *endpoint-windows-info-os*, *endpoint-machine-info*, *endpoint-windows-protected-workspace*

endpoint-check-software

Manages an Endpoint Software Check agent.

Syntax

Configure the **endpoint-check-software** component within the **apm policy agent** module using the following syntax.

Create/Modify

```
create endpoint-check-software [name]
modify endpoint-check-software [name]
    collect [ true | false ]
    continuous-check [ true | false ]
    type  [ antivirus | firewall | patch-management | antispyware | peer-to-peer |
hard-disk-encryption | health-agent ]
    check-list-type [ required | allow | deny ]
    items [ vendor_id | product_id | state | version | db-age | db-version | last-scan
| missing-updates | platform ]
edit endpoint-check-software [ [ [name] | [glob] | [regex] ] ... ]
    all-properties
    non-default-properties
```

Display

```
list endpoint-check-software
list endpoint-check-software [ [ [name] | [glob] | [regex] ] ... ]
show running-config endpoint-check-software
show running-config endpoint-check-software [ [ [name] | [glob] | [regex] ] ... ]
    all
    all-properties
    app-service
    current-module
    non-default-properties
    one-line
    partition
```

Delete

```
delete endpoint-check-software ([name] | all)
```

Description

Endpoint security is a centrally-managed method of monitoring and maintaining client-system security. You can use the *endpoint-check-software* component to create and manage an agent that enforces monitoring of various client-system security third party software. Different *type* s of third party software supported are described below in options.

The configuration attributes in the *items* option are generic and therefore for a given software *type* only certain *items* attributes are useful, rest of the attributes are ignored even if they are configured. For example: for *type* = *peer-to-peer* only *vendor_id*, *product_id*, *state* and *version* are considered and rest of the *items* like *db-age*, *db-version* etc are ignored. Following is the list of useful attributes corresponding to the software *type*:

Commont to all software *type*: *vendor_id*, *product_id*, *version*, *platform*

antivirus & antispyware: *db-age*, *db-version*, *last-scan*, *state*

patch-management: *missing-updates*, *state*

health-agent: *compliant*

hard-disk encryption, Peer-to-peer and firewall: *state*

Examples

- **create endpoint-check-software MyEndpointWCagent items state enabled add**
  Creates the Endpoint Check Software agent named **MyEndpointWCagent**, which
  verifies that the specified third party software on the client is compliant with system administrators configuration, which my just check for the installation or monitor the state of the software
- **list endpoint-check-software**
  Displays a list of Endpoint Software Check agents.
- **delete endpoint-check-software MyEndpointWCagent**
  Deletes the Endpoint Software Check agent named **MyEndpointWCagent**.

Options

- **items**
  Adds items to or deletes items from an Endpoint Software Check agent. You can specify the following attributes for the software:
  - **check-list-type**Specifies how the list of software should be checked
    required: Client is required to have at least one of the software configured in the list in order to pass the access policy. And that software should satisfy all the configuration fields e.g. state, version etc.
    allow: Client is allowed to have any of the software configured in the list but NOT any other than that, in order to pass the access policy. List is treated as whitelist. A given client software will not match unless it satisfies all the configuration fields (e.g. state, version etc).
    NOTE: The check will also be successful if client has no software installed at all. List of software is treated as whitelist.
    deny: Client should NOT have any software configured in the list in order to pass the access policy. And that software should satisfy all

the configuration fields (e.g. state, version etc). *NOTE*: The check will also be successful if client has no software installed at all. List of software is treated as blacklist.

- **db-age**
  Specifies the maximum age of the anti-virus/anti-spyware database that you want an Endpoint Software Check agent to verify the presence of on the client in order to allow the access policy to pass.
- **db-version**
  Specifies the version of the anti-virus/anti-spyware database that you want an Endpoint Software Check agent to verify the presence of on the client in order to allow the access policy to pass.
- **product_id**
  Specifies the product ID of the software that you want an Endpoint Software Check agent to verify the presence of on the client in order to allow the access policy to pass.
- **vendor_id**
  Specifies the vendor ID of the software that you want an Endpoint Software Check agent to verify the presence of on the client in order to allow the access policy to pass.
  NOTE: If none of the vendor id or product id is defined then check is performed for any of the software of given *type* If both vendor id and product id are configured then, product id is ignored and only vendor id is considered. Vendor ID always takes precedence. A vendor can have many products. Each product (of every vendor) has unique ID assigned to them. Similarly, every vendor is assigned a unique ID too which is separate from product ID. If you want to check every software from a vendor then specify *vendor_id* only.
- **state**
  State means different things to different software *type*. The *state* can be *enabled*, *disabled* or *unspecified*. The default is *unspecified*.
  antivirus and *antispyware*: When the *state* is set to *enabled* or *disabled*, agent verifies that the specified antivirus/antispyware software has real time protection enabled or disabled on the client that is attempting to connect. When *state* is *unspecified*, it ignores the *state*.
  patch-management: When the *state* is set to *enabled*, agent verifies that the specified PM software is running on the client that is attempting to connect. When its set to *unspecified*, state of the software is ignored.
  firewall: When the *state* is *enabled* or *disabled*, agent verifies that the specified firewall software has real time protection enabled or disabled on the client that is attempting to connect. When *state* is *unspecified*, the software state is ignored.
  peer-to-peer: When the *state* is set to *enabled* agent verifies that the peer-to-peer software is running on the client that is attempting to connect. When *state* is *unspecified*, the agent only verifies that the software is installed or not.
  hard-disk-encryption: When the *state* is set to *enabled* agent verifies that all disk volumes are encrypted on the client that is attempting to connect. When *state* is *unspecified*, the agent only verifies that the

software is installed or not.
health-agent: When the *state* is set to *enabled* agent verifies that endpoint client is compliant with the health policy set out by the site administrator.

- **version**
  Specifies the version of the software that you want an Endpoint Software Check agent to verify the presence of on the client in order to allow the access policy to pass.
- **last-scan**
  Specifies the maximum allowed duration without the full system scan of endpoint client that software agent can accept in order to allow the access policy to pass. It is specified in number of days.
- **missingupdates**
  Specifies the maximum number of allowed missing critical updates of the PM software at the endpoint client in order to allow the access policy to pass. Leave blank to ignore number of missing critical updates. Specify 0 to make sure endpoint client is up-to-date
- **platform**
  Specifies the platform. It could be any of the following: *windows*, *linux*, *mac* or *any*. The default is *any*.

◆ **type**
Its the type of the third party software to be monitored on the client system. It could be any of the following: *antivirus*, *firewall*, *patch-management*, *antispyware*, *peer-to-peer*, *hard-disk-encryption*, *health-agent*

◆ **collect**
This setting is ignored.

◆ **continuous-check**
Continuously check the *items*, and end the session if the result changes. The default is *false*.

◆ **[name]**
Specifies the name of an Endpoint Software Check agent. This option is required.

◆ **partition**
Displays the partition within which the component resides.

See Also

endpoint-linux-check-file, *endpoint-linux-check-process*, *endpoint-mac-check-file*, *endpoint-mac-check-process*, *endpoint-windows-browser-cache-cleaner*, *endpoint-windows-check-file*, *endpoint-check-machine-cert*, *endpoint-windows-check-process*, *endpoint-windows-check-registry*, *Warning:This page is obsolete. Windows Group Policy is no longer supported. endpoint-windows-group-policy - Manages an Endpoint Windows Group Policy agent.*, *endpoint-windows-info-os*, *endpoint-machine-info*, *endpoint-windows-protected-workspace*

endpoint-linux-check-file

Manages an Endpoint Linux Check File agent.

Syntax

Configure the **endpoint-linux-check-file** component within the **policy agent** module using the following syntax.

Create/Modify

```
create endpoint-linux-check-file [name]
modify endpoint-linux-check-file [name]
    continuous-check [ true | false ]
    app-service [[string] | none]
    files [ filename | md5 | modified | size ]
edit endpoint-linux-check-file [ [ [name] | [glob] | [regex] ] ... ]
    all-properties
    non-default-properties
```

Display

```
list endpoint-linux-check-file
list endpoint-linux-check-file [ [ [name] | [glob] | [regex] ] ... ]
show running-config endpoint-linux-check-file
show running-config endpoint-linux-check-file  [ [ [name] | [glob] | [regex] ] ... ]
    all
    all-properties
    app-service
    current-module
    non-default-properties
    one-line
    partition
```

Delete

```
delete endpoint-linux-check-file ([name] | all)
```

Description

Access Policy Manager checks for the presence of one or more files on a client that is attempting to connect. If a file with the described properties exists, the action goes to the successful branch. If the file does not exist, or a file exists but one or more properties are not correct, the action goes to the fallback branch.

You can use the **endpoint-linux-check-file** component to create or manage an Endpoint Linux Check File agent that verifies the presence of specified Linux files on a client.

Examples

- **create endpoint-linux-check-file Myprofile_act_file_check_ag {**
  files {
  filename "/tmp/demo/demofile"
  md5 "6b61ad518c23650b17e738e1fa2bb04e"
  modified 2007-06-01 10:30:10
  size 12
  }
  {
  filename "/tmp/demo/testfile"
  md5 "f20d9f2072bbeb6691c0f9c5099b01f3"
  size 9
  }
  }
  Creates the Endpoint Linux Check File agent named **Myprofile_act_file_check_ag** that checks that the client contains two files located in the /tmp/demo directory: a 12 byte file named **demofile** that was modified no later than January 6, 2007 at 10:30 and has an MD5 checksum of **6b61ad518c23650b17e738e1fa2bb04e**, and a 9-byte file named **testfile** that has an MD5 check sum of **f20d9f2072bbeb6691c0f9c5099b01f3**.
- **list all endpoint-linux-check-file Company8profile_act_file_check_ag**
  Displays information about the Endpoint Linux Check File agent named Company8profile_act_file_check_ag.
- **delete endpoint-linux-check-file Company8profile_act_check_file { files { filename "/tmp/demo/demofile" }}**
  Deletes the /tmp/demo/demofile file from the Endpoint Linux Check File agent named **Company8profile_act_file_check_ag**.

Options

- **app-service**
  Specifies the name of the application service to which the object belongs. The default value is **none**. **Note:** If the **strict-updates** option is **enabled** on the application service that owns the object, you cannot modify or delete the object. Only the application service can modify or delete the object.
- **files**
  Adds files to or deletes files from an Endpoint Linux Check File agent. You can specify the following attributes of the files that you want an Endpoint Linux Check File agent to verify the presence of on the client in order to allow the access policy to pass.
  - **filename**
    Specifies the name of the file and includes the full path. The Endpoint linus Check File agent that you are creating must be able to verify the file's presence on the client for the access policy to pass. When you add a file to or delete a file from the agent, this setting is required.

- **md5**
  Specifies the value of an MD5 checksum. The Endpoint Linux Check File agent you are creating must be able to match the checksum on the client for the access policy to pass. The default is **none**.
- **modified**
  Specifies the last modified date of the specified file. The Endpoint Linux Check File agent you are creating must verify this date on the client for the access policy to pass. The default is **1970-01-01 00:00:00**.
- **size**
  Specifies the size, in bytes, of the specified file. The Endpoint Linux Check File agent you are creating must verify this size on the client for the access policy to pass. The default is **0**.

◆ **continuous-check**
Continuously check the **files**, and end the session if the result changes. The default is **false**.

◆ **[name]**
Specifies the name of an Endpoint Linux Check File agent. This setting is required.

◆ **partition**
Displays the partition within which the component resides.

See Also

endpoint-check-software, *endpoint-linux-check-process*, *endpoint-mac-check-file*, *endpoint-mac-check-process*, *endpoint-windows-browser-cache-cleaner*, *endpoint-windows-check-file*, *endpoint-check-machine-cert*, *endpoint-windows-check-process*, *endpoint-windows-check-registry*, *endpoint-windows-info-os*, *endpoint-machine-info*, *endpoint-windows-protected-workspace*

endpoint-linux-check-process

Manages an Endpoint Linux Check Process agent.

Syntax

Configure the **endpoint-linux-check-process** component within the **policy agent** module using the following syntax.

Create/Modify

```
create endpoint-linux-check-process [name]
modify endpoint-linux-check-process [name]
  options
    continuous-check [ true | false ]
    app-service [[string] | none]
    expression [ string | none ]
edit endpoint-linux-check-process [ [ [name] | [glob] | [regex] ] ... ]
    all-properties
    non-default-properties
```

Display

```
list endpoint-linux-check-process
list endpoint-linux-check-process [ [ [name] | [glob] | [regex] ] ... ]
show running-config endpoint-linux-check-process
show running-config endpoint-linux-check-process  [ [ [name] | [glob] | [regex] ] ...
]
    all
    all-properties
    app-service
    current-module
    non-default-properties
    one-line
    partition
```

Delete

```
delete endpoint-linux-check-process [name]
```

Description

You can use the **endpoint-linux-check-process** component to create and manage an Endpoint Linux Check Process agent that collects information about the Linux processes running on the client.

Examples

- **create endpoint-linux-check-process MyEndpointWCPagent { (bash OR top) AND firefox }**
  Creates the Endpoint Linux Check Process agent named **MyEndpointWCPagent** that checks that the client has either bash or top, and firefox launched.
- **list endpoint-linux-check-process**
  Displays a list of Endpoint Linux Check Process agents.
- **delete endpoint-linux-check-process MyEndpointWCPagent**
  Deletes the Endpoint Linux Check Process agent named **MyEndpointWCPagent**.

Options

- **app-service**
  Specifies the name of the application service to which the object belongs. The default value is **none**. **Note:** If the **strict-updates** option is **enabled** on the application service that owns the object, you cannot modify or delete the object. Only the application service can modify or delete the object.
- **expression**
  Specifies the expression that you want an Endpoint Linux Check Process agent to use to verify the processes that are running on the client to allow the access policy to pass. You can use the following operators: AND, OR, NOT, (and). You can use wildcards in the process name, for example, navapsvc.*.
  If the check is successful, the system returns **1**. If the check fails, the system returns **0**. If the expression is incorrect, the system returns **-1**.
- **continuous-check**
  Continuously check the **expression**, and end the session if the result changes. The default is **false**.
- **[name]**
  Specifies the name of an Endpoint Linux Check Process agent. This setting is required.
- **partition**
  Displays the partition within which the component resides.

See Also

endpoint-check-software, *endpoint-linux-check-file*, *endpoint-mac-check-file*, *endpoint-mac-check-process*, *endpoint-windows-browser-cache-cleaner*, *endpoint-windows-check-file*, *endpoint-check-machine-cert*, *endpoint-windows-check-process*, *endpoint-windows-check-registry*, *Warning:This page is obsolete. Windows Group Policy is no longer supported. endpoint-windows-group-policy - Manages an Endpoint Windows Group Policy agent.*,

endpoint-windows-info-os, *endpoint-machine-info*, *endpoint-windows-protected-workspace*

endpoint-mac-check-file

Manages an Endpoint Macintosh Check File agent.

Syntax

Configure the **endpoint-mac-check-file** component within the **policy agent** module using the following syntax.

Create/Modify

```
create endpoint-mac-check-file  [name]
modify endpoint-mac-check-file  [name]
  options
    continuous-check [ true | false ]
    app-service [[string] | none]
    files [ filename | md5 | modified | size ]
edit endpoint-mac-check-file [ [ [name] | [glob] | [regex] ] ... ]
    all-properties
    non-default-properties
```

Display

```
list endpoint-mac-check-file
list endpoint-mac-check-file  [ [ [name] | [glob] | [regex] ] ... ]
show running-config endpoint-mac-check-file
show running-config endpoint-mac-check-file   [ [ [name] | [glob] | [regex] ] ... ]
    all
    all-properties
    app-service
    current-module
    non-default-properties
    one-line
    partition
```

Delete

```
delete endpoint-mac-check-file  ([name] | all)
```

Description

Access Policy Manager checks for the presence of one or more files on a client that is attempting to connect. If a file with the described properties exists, the action goes to the successful branch. If the file does not exist, or a file exists but one or more properties are not correct, the action goes to the fallback branch.

You can use the **endpoint-mac-check-file** component to create or manage an Endpoint Macintosh Check File agent that verifies the presence of specified Macintosh files on a client.

Examples

- **create endpoint-mac-check-file Myprofile_act_file_check_ag {**
  files {
  filename "/tmp/demo/demofile"
  md5 "6b61ad518c23650b17e738e1fa2bb04e"
  modified 2007-06-01 10:30:10
  size 12
  }
  {
  filename "/tmp/demo/testfile"
  md5 "f20d9f2072bbeb6691c0f9c5099b01f3"
  size 9
  }
  }
  Creates the Endpoint Macintosh Check File agent named **Myprofile_act_file_check_ag** that checks that the client contains two files located in the /tmp/demo directory: a 12 byte file named **demofile** that was modified no later than January 6, 2007 at 10:30 and has an MD5 checksum of **6b61ad518c23650b17e738e1fa2bb04e**, and a 9 byte file named **testfile** that has an MD5 check sum of **f20d9f2072bbeb6691c0f9c5099b01f3**.
- **list all endpoint-mac-check-file Company8profile_act_file_check_ag**
  Displays information about the Endpoint Macintosh Check File agent named Company8profile_act_file_check_ag.
- **delete endpoint-mac-check-file Company8profile_act_check_file { files { filename "/tmp/demo/demofile" }}**
  Deletes the /tmp/demo/demofile file from the Endpoint Macintosh Check File agent named **Company8profile_act_file_check_ag**.

Options

- **app-service**
  Specifies the name of the application service to which the object belongs. The default value is **none**. **Note:** If the **strict-updates** option is **enabled** on the application service that owns the object, you cannot modify or delete the object. Only the application service can modify or delete the object.
- **files**
  Adds files to or deletes files from an Endpoint Macintosh Check File agent. You can specify the following attributes of the files that you want an Endpoint Macintosh Check File agent to verify the presence of on the client to allow the access policy to pass:
  - **filename**
    Specifies the name of the file and includes the full path. The Endpoint Macintosh Check File agent that you are creating must be able to verify the file's presence on the client for the access policy to pass. When you add a file to or delete a file from the agent, this setting is required.

- **md5**
  Specifies the value of an MD5 checksum. The Endpoint Macintosh Check File agent you are creating must be able to match the checksum on the client for the access policy to pass. The default is **none**.
- **modified**
  Specifies the last modified date of the specified file. The Endpoint Macintosh Check File agent you are creating must verify this date on the client for the access policy to pass. The default is **1970-01-01 00:00:00**.
- **size**
  Specifies the size, in bytes, of the specified file. The Endpoint Macintosh Check File agent you are creating must verify this size on the client for the access policy to pass. The default is **0**.

◆ **continuous-check**
Continuously check the **files**, and end the session if the result changes. The default is **false**.

◆ **[name]**
Specifies the name of an Endpoint Macintosh Check File agent. This setting is required.

◆ **partition**
Displays the partition within which the component resides.

See Also

endpoint-check-software, *endpoint-linux-check-file*, *endpoint-linux-check-process*, *endpoint-mac-check-process*, *endpoint-windows-browser-cache-cleaner*, *endpoint-windows-check-file*, *endpoint-check-machine-cert*, *endpoint-windows-check-process*, *endpoint-windows-check-registry*, *Warning:This page is obsolete. Windows Group Policy is no longer supported. endpoint-windows-group-policy - Manages an Endpoint Windows Group Policy agent.*, *endpoint-windows-info-os*, *endpoint-machine-info*, *endpoint-windows-protected-workspace*

endpoint-mac-check-process

Manages an Endpoint Macintosh Check Process agent.

Syntax

Configure the **endpoint-mac-check-process** component within the **policy agent** module using the following syntax.

Create/Modify

```
create endpoint-mac-check-process [name]
modify endpoint-mac-check-process [name]
  options
    continuous-check [ true | false ]
    app-service [[string] | none]
    expression [ string | none ]
edit endpoint-mac-check-process [ [ [name] | [glob] | [regex] ] ... ]
     all-properties
     non-default-properties
```

Display

```
list endpoint-mac-check-process
list endpoint-mac-check-process [ [ [name] | [glob] | [regex] ] ... ]
show running-config endpoint-mac-check-process
show running-config endpoint-mac-check-process  [ [ [name] | [glob] | [regex] ] ... ]
    all
    all-properties
    app-service
    current-module
    non-default-properties
    one-line
    partition
```

Delete

```
delete endpoint-mac-check-process ([name] | all)
```

Description

You can use the **endpoint-mac-check-process** component to create and manage an Endpoint Macintosh Check Process agent that collects information about the Macintosh processes running on the client.

Examples

- **create endpoint-mac-check-process MyEndpointWCPagent { (bash OR top) AND firefox }**
  Creates the Endpoint Macintosh Check Process agent named **MyEndpointWCPagent** that checks that the client has either bash or top, and firefox launched.
- **list endpoint-mac-check-process**
  Displays a list of Endpoint Macintosh Check Process agents.
- **delete endpoint-mac-check-process MyEndpointWCPagent**
  Deletes the Endpoint Macintosh Check Process agent named **MyEndpointWCPagent**.

Options

- **app-service**
  Specifies the name of the application service to which the object belongs. The default value is **none**. **Note:** If the **strict-updates** option is **enabled** on the application service that owns the object, you cannot modify or delete the object. Only the application service can modify or delete the object.
- **expression**
  Specifies the expression that you want an Endpoint Macintosh Check Process agent to use to verify the processes that are running on the client in order to allow the access policy to pass. You can use the following operators: AND, OR, NOT, (and). You can use wildcards in the process name, for example, navapsvc.*.
  If the check is successful, the system returns **1**. If the check fails, the system returns **0**. If the expression is incorrect, the system returns **-1**.
- **continuous-check**
  Continuously check the **expression**, and end the session if the result changes. The default is **false**.
- **[name]**
  Specifies the name of an Endpoint Macintosh Check Process agent. This setting is required.
- **partition**
  Displays the partition within which the component resides.

endpoint-machine-info

Manages an Endpoint Machine Information agent.

Syntax

Configure the **endpoint-machine-info** component within the **policy agent** module using the following syntax.

Create/Modify

```
create endpoint-machine-info [name]
modify endpoint-machine-info [name]
    app-service [[string] | none]
edit endpoint-machine-info [ [ [name] | [glob] | [regex] ] ... ]
    all-properties
    non-default-properties
    one-line
```

Display

```
list endpoint-machine-info
list endpoint-machine-info [ [ [name] | [glob] | [regex] ] ... ]
show running-config endpoint-machine-info
show running-config endpoint-machine-info [ [ [name] | [glob] | [regex] ] ... ]
    all-properties
    non-default-properties
    partition
show endpoint-machine-info
show endpoint-machine-info [name]
```

Delete

```
delete endpoint-machine-info [name]
```

Description

You can use the **endpoint-machine-info** component to create and manage an agent that collects information about the machine that is attempting to connect.

Options

- **[name]**
  Specifies the name of the an Endpoint Check Machine Information agent. This setting is required.
- **partition**
  Displays the partition within which the component resides.

- **app-service**
  Specifies the name of the application service to which the object belongs. The default value is **none**. **Note:** If the **strict-updates** option is **enabled** on the application service that owns the object, you cannot modify or delete the object. Only the application service can modify or delete the object.

See Also

endpoint-check-software, *endpoint-linux-check-file*, *endpoint-linux-check-process*, *endpoint-mac-check-file*, *endpoint-mac-check-process*, *endpoint-windows-browser-cache-cleaner*, *endpoint-windows-check-file*, *endpoint-check-machine-cert*, *endpoint-windows-check-process*, *endpoint-windows-check-registry*, *Warning:This page is obsolete. Windows Group Policy is no longer supported. endpoint-windows-group-policy - Manages an Endpoint Windows Group Policy agent.*, *endpoint-windows-info-os*, *endpoint-windows-protected-workspace*

endpoint-windows-browser-cache-cleaner

Manages an Endpoint Windows Browser Cache Cleaner agent.

Syntax

Configure the **endpoint-windows-browser-cache-cleaner** component within the **policy agent** module using the following syntax.

Create/Modify

```
create endpoint-windows-browser-cache-cleaner  [name]
modify endpoint-windows-browser-cache-cleaner  [name]
  options
     app-service [[string] | none]
     cache-clean-type [all | all-except-css-js | all-except-img-css-js | none ]
     clean-passwords [false | true ]
     empty-recycle-bin [false | true ]
     idle-timeout [<integer> | immediate | indefinite]
     idle-timeout-screen-lock [<integer>]
     monitor-webtop [enable | disable]
     partition <name>
     remove-connection-entry [false | true ]
edit endpoint-windows-browser-cache-cleaner [ [ [name] | [glob] | [regex] ] ... ]
   all-properties
   non-default-properties
```

Display

```
list endpoint-windows-browser-cache-cleaner
list endpoint-windows-browser-cache-cleaner  [ [ [name] | [glob] | [regex] ] ... ]
show running-config endpoint-windows-browser-cache-cleaner
show running-config endpoint-windows-browser-cache-cleaner   [ [ [name] | [glob] |
[regex] ] ... ]
    all
    all-properties
    app-service
    current-module
    non-default-properties
    one-line
    partition
```

Delete

```
delete endpoint-windows-browser-cache-cleaner  ([name] | all)
```

Description

Endpoint security is a centrally-managed method of monitoring and maintaining client-system security. You can use the **endpoint-windows-browser-cache-cleaner** component to create and

manage an Endpoint Windows Browser Cache Cleaner agent. This agent cleans items from the client browser and computer after logoff, and also enforces session inactivity timeouts.

Examples

- **create endpoint-windows-browser-cache-cleaner MyEndpointWBCCagent idle timeout 0**
  Creates the Endpoint Windows Browser Cache Cleaner agent named **MyEndpointWBCCagent** that does not enforce a timeout.
- **create endpoint-windows-browser-cache-cleaner MyEndpointWBCCagent { idle timeout 0 clean passwords enable }**
  Creates the Endpoint Windows Browser Cache Cleaner agent named **MyEndpointWBCCagent** that does not enforce a timeout, but does clear saved passwords from the client after logoff.
- **list endpoint-windows-browser-cache-cleaner**
  Displays a list of Endpoint Windows Browser Cache Cleaner agents.
- **delete endpoint-windows-browser-cache-cleaner MyEndpointWBCCagent**
  Deletes the Endpoint Windows Browser Cache Cleaner agent named **MyEndpointWBCCagent**.

Options

- **app-service**
  Specifies the name of the application service to which the object belongs. The default value is **none**. **Note:** If the **strict-updates** option is **enabled** on the application service that owns the object, you cannot modify or delete the object. Only the application service can modify or delete the object.
- **cache-clean-type**
  Specifies which browser cache temporary files are removed. If set to **all**, the temporary files are removed. If set to **all-except-css-js**, the browser cache is cleared, but all style sheets and JavaScript are left on the browser cache. If set to **all-except-img-css-js**, the browser cache is cleared, but all style sheets, JavaScript, and images are left on the browser cache. The default is **all**.
- **clean-passwords**
  When **true**, the Endpoint Windows Browser Cache Cleaner agent ensures that saved passwords are cleared from the client after logoff. The default is **false**.
- **empty-recycle-bin**
  When **true**, the Endpoint Windows Browser Cache Cleaner agent empties the Recycle Bin on the client after logoff. The default is **false**.

- **idle-timeout**
  Specifies the number of minutes that the client session can be idle before the Endpoint Windows Browser Cache Cleaner agent disconnects the session. The default is **0**, which enforces no timeout. This is a required setting.
- **Idle-timeout-screen-lock**
  Specifies the number of minutes the system can receive no user input before the workstation is locked. The default is **0**, which specifies no timeout enforced.
- **monitor-webtop**
  When **true**, the Endpoint Windows Browser Cache Cleaner agent forces session termination if the browser or webtop is closed. The default is **false**.
- **[name]**
  Specifies the name of the Endpoint Windows Browser Cache Cleaner agent. This is a required setting.
- **partition**
  Displays the partition within which the component resides.
- **remove-connection-entry**
  When **true**, the Endpoint Windows Browser Cache Cleaner agent removes the connection from the Network Connections Dial-up Networking folder on the client. The default is **false**.

See Also

endpoint-check-software, *endpoint-linux-check-file*, *endpoint-linux-check-process*, *endpoint-mac-check-file*, *endpoint-mac-check-process*, *endpoint-windows-check-file*, *endpoint-check-machine-cert*, *endpoint-windows-check-process*, *endpoint-windows-check-registry*, *endpoint-windows-info-os*, *endpoint-machine-info*, *endpoint-windows-protected-workspace*

endpoint-windows-check-file

Manages an Endpoint Windows Check File agent.

Syntax

Configure the **endpoint-windows-check-file** component within the **policy agent** module using the following syntax.

Create/Modify

```
create endpoint-windows-check-file  [name]
modify endpoint-windows-check-file  [name]
  options
    continuous-check [ true | false ]
    app-service [[string] | none]
    files [ filename | md5 | modified | operation | signer | size | version ]
edit endpoint-windows-check-file [ [ [name] | [glob] | [regex] ] ... ]
    all-properties
    non-default-properties
```

Display

```
list endpoint-windows-check-file
list endpoint-windows-check-file  [ [ [name] | [glob] | [regex] ] ... ]
show running-config endpoint-windows-check-file
show running-config endpoint-windows-check-file   [ [ [name] | [glob] | [regex] ] ...
]
    all
    all-properties
    app-service
    current-module
    non-default-properties
    one-line
    partition
```

Delete

```
delete endpoint-windows-check-file  ([name] | all)
```

Description

Access Policy Manager checks for the presence of one or more files on a client that is attempting to connect. If a file with the described properties exists, the action goes to the successful branch. If the file does not exist, or a file exists but one or more properties are not correct, the action goes to the fallback branch.

You can use the **endpoint-windows-check-file** component to create or manage an Endpoint Windows Check File agent that verifies the presence of specified Windows files on a client.

Examples

- **create endpoint-windows-check-file Myprofile_act_file_check_ag {**
  files {
  filename "C:\demo\demofile"
  md5 "6b61ad518c23650b17e738e1fa2bb04e"
  modified 2007-06-01 10:30:10
  size 12
  }
  {
  filename "C:\demo\test.file"
  md5 "f20d9f2072bbeb6691c0f9c5099b01f3"
  size 9
  }
  }
  Creates the Endpoint Windows Check File agent named **Myprofile_act_file_check_ag** that checks that the client contains two files located in the C:demo directory: a 12 byte file named **demofile** that was modified no later than **January 6, 2007 at 10:30** and has an MD5 checksum of **6b61ad518c23650b17e738e1fa2bb04e**, and a 9 byte file named **test.file** that has an MD5 check sum of **f20d9f2072bbeb6691c0f9c5099b01f3**.
- **list all endpoint-windows-check-file Company8profile_act_file_check_ag**
  Displays information about the Endpoint Windows Check File agent named **Company8profile_act_file_check_ag**.
- **delete endpoint-windows-check-file Company8profile_act_check_file { files { filename "C:\demo\demofile" }}**
  Deletes the C:demodemofile file from the Endpoint Windows Check File agent named **Company8profile_act_file_check_ag**.

Options

- **app-service**
  Specifies the name of the application service to which the object belongs. The default value is **none**. **Note:** If the **strict-updates** option is **enabled** on the application service that owns the object, you cannot modify or delete the object. Only the application service can modify or delete the object.
- **files**
  Adds files to or deletes files from an Endpoint Windows Check File agent. You can specify the following attributes for the files that you want an Endpoint Windows Check File agent to verify the presence of on the client to allow the access policy to pass.
  - **filename**
    Specifies a file name and includes the full path. The Endpoint windows Check File agent you are creating must be able to verify the file's presence on the client for the access policy to pass. When you add a file to or delete a file from the agent, this setting is required.

- **md5**
  Specifies the value of an MD5 checksum. The Endpoint windows Check File agent that you are creating must match the checksum on the client for the access policy to pass. The default is **none**.
- **modified**
  Specifies the last modified date of the specified file. The Endpoint windows Check File agent you are creating must verify this date on the client for the access policy to pass. The default is **1970-01-01 00:00:00**.
- **operation**
  Specifies the operator that you want your Endpoint Windows Check File agent to use when verifying the attributes of the specified file on the client. The default is **equal**.
- **signer**
  Specifies that the Endpoint Windows Check File agent must verify that the specified file on the client is signed for the access policy to pass. The default is **none**.
- **size**
  Specifies the size, in bytes, of the specified file. The Endpoint Windows Check File agent you are creating must verify this file size on the client for the access policy to pass. The default is **0**.
- **version**
  Specifies the version of the specified file that you want your Endpoint Windows Check File agent to verify on the client for the access policy to pass. Specify the version using the followoiong form: **x.x.x.x**. The maximum value is **65535.65535.65535.65535**. The default is **none**.

◆ **continuous-check**
Continuously check the **files**, and end the session if the result changes. The default is **false**.

◆ **[name]**
Specifies the name of an Endpoint Windows Check File agent. This option is required.

◆ **partition**
Displays the partition within which the component resides.

See Also

endpoint-check-software, *endpoint-linux-check-file*, *endpoint-linux-check-process*, *endpoint-mac-check-file*, *endpoint-mac-check-process*, *endpoint-windows-check-file*, *endpoint-windows-browser-cache-cleaner*, *endpoint-windows-check-process*, *endpoint-windows-check-registry*, *Warning:This page is obsolete. Windows Group Policy is no longer supported. endpoint-windows-group-policy - Manages an Endpoint Windows Group Policy agent.*, *endpoint-windows-info-os*, *endpoint-machine-info*, *endpoint-windows-protected-workspace*

endpoint-windows-check-process

Manages an Endpoint Windows Check Process agent.

Syntax

Configure the **endpoint-windows-check-process** component within the **policy agent** module using the following syntax.

Create/Modify

```
create endpoint-windows-check-process [name]
modify endpoint-windows-check-process [name]
    continuous-check [ true | false ]
    app-service [[string] | none]
    expression (<string> | none)
edit endpoint-windows-check-process [ [ [name] | [glob] | [regex] ] ... ]
    all-properties
    non-default-properties
```

Display

```
list endpoint-windows-check-process
list endpoint-windows-check-process [ [ [name] | [glob] | [regex] ] ... ]
show running-config endpoint-windows-check-process
show running-config endpoint-windows-check-process [ [ [name] | [glob] | [regex] ] ...
]
    all-properties
    non-default-properties
    partition
show endpoint-windows-check-process
show endpoint-windows-check-process [name]
```

Delete

```
delete endpoint-windows-check-process [name]
```

Description

You can use the **endpoint-windows-check-process** component to create and manage an agent that collects information about the Windows processes running on the client.

Examples

- **create endpoint-windows-check-process MyEndpointWCPagent { (NISUM.exe OR blackd.exe) AND navapsvc.* }**
  Creates the Endpoint Windows Check Process agent named **MyEndpointWCPagent** that checks that the client has either NISUM.exe or blackd.exe, and navapsvc.* installed.
- **list endpoint-windows-check-process**
  Displays a list of Endpoint Windows Check Process agents.
- **delete endpoint-windows-check-process MyEndpointWCPagent delete**
  Deletes the Endpoint Windows Check Process agent named **MyEndpointWCPagent**.

Options

- **app-service**
  Specifies the name of the application service to which the object belongs. The default value is **none**. **Note:** If the **strict-updates** option is **enabled** on the application service that owns the object, you cannot modify or delete the object. Only the application service can modify or delete the object.
- **expression**
  Specifies the expression that you want an Endpoint Windows Check Process agent to use to verify the processes that are running on the client in order to allow the access policy to pass. You can use the following operators: AND, OR, NOT, (and). You can use wildcards in the process name, for example, navapsvc.*.
  If the check is successful, the system returns **1**. If the check fails, the system returns **0**. If the expression is incorrect, the system returns **-1**.
- **continuous-check**
  Continuously check the **expression**, and end the session if the result changes. The default is **false**.
- **[name]**
  Specifies the name of an Endpoint Windows Check Process agent. This setting is required.
- **partition**
  Displays the partition within which the component resides.

See Also

endpoint-check-software, *endpoint-linux-check-file*, *endpoint-linux-check-process*, *endpoint-mac-check-file*, *endpoint-mac-check-process*, *endpoint-windows-check-file*, *endpoint-check-machine-cert*, *endpoint-windows-browser-cache-cleaner*, *endpoint-windows-check-registry*, *Warning:This page is obsolete. Windows Group Policy is no longer supported. endpoint-windows-group-policy -*

Manages an Endpoint Windows Group Policy agent., *endpoint-windows-info-os*, *endpoint-machine-info*, *endpoint-windows-protected-workspace*

endpoint-windows-check-registry

Manages an Endpoint Windows Check Registry agent.

Syntax

Configure the **endpoint-windows-check-registry** component within the **policy agent** module using the following syntax.

Create/Modify

```
create endpoint-windows-check-registry [name]
modify endpoint-windows-check-registry [name]
    continuous-check [ true | false ]
    app-service [[string] | none]
    expression [[string] | none]
edit endpoint-windows-check-registry [ [ [name] | [glob] | [regex] ] ... ]
    all-properties
    non-default-properties
```

Display

```
list endpoint-windows-check-registry
list endpoint-windows-check-registry [ [ [name] | [glob] | [regex] ] ... ]
show running-config endpoint-windows-check-registry
show running-config endpoint-windows-check-registry [ [ [name] | [glob] | [regex] ]
... ]
    all-properties
    non-default-properties
    partition
show endpoint-windows-check-registry
show endpoint-windows-check-registry [name]
```

Delete

```
delete endpoint-windows-check-registry [name]
```

Description

You can use the **endpoint-windows-check-registry** component to create and manage an agent that collects information about the Windows registry keys on the client that is attempting to connect.

Examples

- **create endpoint-windows-check-registry MyEndpointWCRagent {""'HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Internet Explorer"."Version"="5.0.2800.0"'" }**
  Creates the Endpoint Windows Check Registry agent named

MyEndpointWCRagent that checks the registry on the client for version 5.0.2800.0 of Internet Explorer in the HKEY_LOCAL_MACHINESOFTWAREMicrosoft directory.

- **create endpoint-windows-check-registry MyEndpointWCRagent {""'HKEY_LOCAL_MACHINE64\SOFTWARE\Microsoft\Internet Explorer"."Version"="5.0.2800.0"'"**
  Creates the Endpoint Windows Check Registry agent named MyEndpointWCRagent that checks the registry on the client for version 5.0.2800.0 of Internet Explorer in the HKEY_LOCAL_MACHINE64SOFTWAREMicrosoft directory.
  Note that the registry value HKEY_LOCAL_MACHINE64 is one of the 32 and 64-bit registry keys that you can specify on 64-bit Windows versions.
  On 64-bit Windows systems, you can check for registry keys in either the 64-bit registry or the 32-bit registry. To specify the registry to check, append a number to the registry root key name. The following key names are supported:
  HKEY_CURRENT_USER
  HKEY_CURRENT_USER32
  HKEY_CURRENT_USER64
  HKEY_LOCAL_MACHINE
  HKEY_LOCAL_MACHINE32
  HKEY_LOCAL_MACHINE64
  HKEY_CLASSES_ROOT
  HKEY_CLASSES_ROOT32
  HKEY_CLASSES_ROOT64
  HKEY_USERS
  HKEY_USERS32
  HKEY_USERS64
  HKEY values specified with a 32 allow you to check values in the 32-bit view of 64-bit registry. This is the perspective used by 32-bit applications running with on a 64-bit operating system.
  HKEY values with a 64 appended allow you to check values in the 64-bit view of the registry. This is the perspective used by native 64-bit applications. When checking values on 32-bit Windows, the number of bits specified in the registry key name is ignored.
- **list endpoint-windows-check-registry**
  Displays a list of Endpoint Windows Check Registry agents.
- **delete endpoint-windows-check-registry MyEndpointWCRagent delete**
  Deletes the Endpoint Windows Check Registry agent named **MyEndpointWCRagent**.

Options

- **app-service**
  Specifies the name of the application service to which the object belongs. The default value is **none**. **Note:** If the **strict-updates** option is **enabled**

on the application service that owns the object, you cannot modify or delete the object. Only the application service can modify or delete the object.

- **expression**
  Specifies the expression that you want an Endpoint Windows Check Registry agent to use to verify the registry entries that are present on the client in order to allow the access policy to pass. You can use the following operators: AND, OR, NOT, (and).
  If the check is successful, the system returns **1**. If the check fails, the system returns **0**. If the expression is incorrect, the system returns **-1**.

Important

You must use quotation marks (" ") around key and value arguments, and in data when the content contains spaces, commas, slashes, tabs, or other delimiters. If quotation marks exist as part of a registry path or value name, you must use quotation marks around those quotation marks.
Tip: *The system treats data in the formats "d.d[.d][.d]" or "d,d[,d][,d]" (where d is a number) as a version number. The system treats data in the format "mm/dd/yyyy" as a date.*

- **continuous-check**
  Continuously check the **expression**, and end the session if the result changes. The default is **false**.
- **[name]**
  Specifies the name of the an Endpoint Windows Check Registry agent. This option is required.
- **partition**
  Displays the partition within which the component resides.

See Also

endpoint-check-software, *endpoint-linux-check-file*, *endpoint-linux-check-process*, *endpoint-mac-check-file*, *endpoint-mac-check-process*, *endpoint-windows-browser-cache-cleaner*, *endpoint-windows-check-file*, *endpoint-check-machine-cert*, *endpoint-windows-check-process*, *Warning:This page is obsolete. Windows Group Policy is no longer supported. endpoint-windows-group-policy - Manages an Endpoint Windows Group Policy agent.*, *endpoint-windows-info-os*, *endpoint-machine-info*, *endpoint-windows-protected-workspace*

Warning: This page is obsolete. Windows Group Policy is no longer supported. endpoint-windows-group-policy - Manages an Endpoint Windows Group Policy agent.

Syntax

Configure the **external-logon-page** component within the **policy agent** module using the following syntax.

Create/Modify

```
create endpoint-windows-group-policy [name]
modify endpoint-windows-group-policy [name]
    app-service [[string] | none]
    policy-file { [name] }
edit endpoint-windows-group-policy [ [ [name] | [glob] | [regex] ] ... ]
    all-properties
    non-default-properties
```

Display

```
list endpoint-windows-group-policy
list endpoint-windows-group-policy [ [ [name] | [glob] | [regex] ] ... ]
show running-config endpoint-windows-group-policy
show running-config endpoint-windows-group-policy [ [ [name] | [glob] | [regex] ] ...
]
    all-properties
    non-default-properties
    partition
show endpoint-windows-group-policy
show endpoint-windows-group-policy [name]
```

Delete

```
delete endpoint-windows-group-policy [name]
```

Description

Endpoint Windows Group Policy agents enable you to apply an Endpoint Windows Group Policy to a client machine and create a result session variable.

Examples

- **create endpoint-windows-group-policy { Firewall_Settings_Template }**
  Creates a policy for the Access Policy using the Firewall Settings template.
- **edit endpoint-windows-group-policy Firewall_Settings_Template**
  Edits the Firewall Settings Template.

Options

- **[name]**
  Specifies a name for the Endpoint Windows Group Policy agent.
- **partition**
  Displays the partition within which the component resides.
- **app-service**
  Specifies the name of the application service to which the object belongs. The default value is **none**. **Note:** If the **strict-updates** option is **enabled** on the application service that owns the object, you cannot modify or delete the object. Only the application service can modify or delete the object.
- **policy-file**
  Specifies the group policy template that is applied to the client. This option is required.

See Also

endpoint-check-software, *endpoint-linux-check-file*, *endpoint-linux-check-process*, *endpoint-mac-check-file*, *endpoint-mac-check-process*, *endpoint-windows-browser-cache-cleaner*, *endpoint-windows-check-file*, *endpoint-check-machine-cert*, *endpoint-windows-check-process*, *endpoint-windows-check-registry*, *endpoint-windows-info-os*, *endpoint-machine-info*, *endpoint-windows-protected-workspace*

endpoint-windows-info-os

Manages an Endpoint Windows Information Operating System agent.

Syntax

Configure the **endpoint-windows-info-os** component within the **policy agent** module using the following syntax.

Create/Modify

```
create endpoint-windows-info-os [name]
modify endpoint-windows-info-os [name]
    app-service [[string] | none]
edit endpoint-windows-info-os [ [ [name] | [glob] | [regex] ] ... ]
    all-properties
    non-default-properties
```

Display

```
list endpoint-windows-info-os
list endpoint-windows-info-os [ [ [name] | [glob] | [regex] ] ... ]
show running-config endpoint-windows-info-os
show running-config endpoint-windows-info-os [ [ [name] | [glob] | [regex] ] ... ]
    all-properties
    non-default-properties
    partition
show endpoint-windows-info-os
show endpoint-windows-info-os [name]
```

Delete

```
delete endpoint-windows-info-os [name]
```

Description

You can use the **endpoint-windows-info-os** component to create and manage an agent that retrieves information about the Microsoft Windows operating system from the client, such as version and hotfix number.

Examples

- **create endpoint-windows-info-os MyEndpointWIOSagent { }**
  Creates the Endpoint Windows Operating System Information agent named **MyEndpointWIOSagent**.
- **list endpoint-windows-info-os**
  Displays a list of Endpoint Windows Operating System Information agents.

- **delete endpoint-windows-info-os MyEndpointWIOSagent delete**
  Deletes the Endpoint Windows Operating System Information agent named **MyEndpointWCRagent**.

Options

- **[name]**
  Specifies the name of an Endpoint Windows Info OS agent. This setting is required.
- **partition**
  Displays the partition within which the component resides.
- **app-service**
  Specifies the name of the application service to which the object belongs. The default value is **none**. **Note:** If the **strict-updates** option is **enabled** on the application service that owns the object, you cannot modify or delete the object. Only the application service can modify or delete the object.

See Also

endpoint-check-software, *endpoint-linux-check-file*, *endpoint-linux-check-process*, *endpoint-mac-check-file*, *endpoint-mac-check-process*, *endpoint-windows-browser-cache-cleaner*, *endpoint-windows-check-file*, *endpoint-check-machine-cert*, *endpoint-windows-check-process*, *endpoint-windows-check-registry*, *Warning:This page is obsolete. Windows Group Policy is no longer supported. endpoint-windows-group-policy - Manages an Endpoint Windows Group Policy agent.*, *endpoint-machine-info*, *endpoint-windows-protected-workspace*

endpoint-windows-protected-workspace

Manages an Endpoint Windows Protected Workspace agent.

Syntax

Configure the **endpoint-windows-protected-workspace** component within the **policy agent** module using the following syntax.

Create/Modify

```
create endpoint-windows-protected-workspace [name]
modify endpoint-windows-protected-workspace [name]
    allow-burn-cid [true | false]
    allow-printer-use [true | false]
    allow-user-switch [true | false]
    allowed-network-shares [add | delete | modify | replace-all-with] {
      [[string]]
    }
    app-service [[string] | none]
    close-google-desktop-search [true | false]
    usb-flash-access [all | ironkey | none]
edit endpoint-windows-protected-workspace [ [ [name] | [glob] | [regex] ] ... ]
    all-properties
    non-default-properties
```

Display

```
list endpoint-windows-protected-workspace
list endpoint-windows-protected-workspace [ [ [name] | [glob] | [regex] ] ... ]
show running-config endpoint-windows-protected-workspace
show running-config endpoint-windows-protected-workspace [ [ [name] | [glob] | [regex]
] ... ]
    all-properties
    non-default-properties
    partition
show endpoint-windows-protected-workspace
show endpoint-windows-protected-workspace [name]
```

Delete

```
delete endpoint-windows-protected-workspace [name]
```

Description

You can use the **endpoint-windows-protected-workspace** component to create and manage an agent that enables an administrator to impose limitations on applications running on Windows client machines.

Options

- **allow-burn-cid**
  Specifies that the user can burn CDs from within protected workspace. The default is **false**.
- **allow-printer-use**
  Specifies whether a user can print inside a protected workspace. The default is **true**.
- **allow-user-switch**
  Specifies whether a user can temporarily switch from a protected workspace. The default is **true**.
- **allowed-network-shares**
  Specifies a list of Windows network shares to which user has Write access. The default is **none**.
- **app-service**
  Specifies the name of the application service to which the object belongs. The default value is **none**. **Note:** If the **strict-updates** option is **enabled** on the application service that owns the object, you cannot modify or delete the object. Only the application service can modify or delete the object.
- **[name]**
  Specifies the name of the Endpoint Windows Protected Workspace agent. This option is required.
- **partition**
  Displays the partition within which the component resides.
- **usb-flash-access**
  Specifies whether a user has access to a USB port. The default is **false**.

See Also

endpoint-check-software, *endpoint-linux-check-file*, *endpoint-linux-check-process*, *endpoint-mac-check-file*, *endpoint-mac-check-process*, *endpoint-windows-browser-cache-cleaner*, *endpoint-windows-check-file*, *endpoint-check-machine-cert*, *endpoint-windows-check-process*, *endpoint-windows-check-registry*, *endpoint-windows-info-os*, *endpoint-machine-info*

external-logon-page

Manages an External Logon Page agent.

Syntax

Configure the **external-logon-page** component within the **policy agent** module using the following syntax.

Create/Modify

```
create external-logon-page [name]
modify external-logon-page [name]
    app-service [[string] | none]
    split-username [true | false]
    uri [[string]> | none]
edit external-logon-page [ [ [name] | [glob] | [regex] ] ... ]
    all-properties
    non-default-properties
```

Display

```
list external-logon-page
list external-logon-page [ [ [name] | [glob] | [regex] ] ... ]
    all-properties
    non-default-properties
    partition
```

Delete

```
delete external-logon-page [name]
```

Description

The External Logon Page agent creates an external Logon page that redirects the client browser.

Examples

- **create external-logon-page MyExternalLogonPageAgent { uri "MyExternalLogonPageServerURI" }**
  Creates the External Logon Page agent named **MyExternalLogonPageAgent** that is associated with the URI **MyExternalLogonPageServerURI**.
- **create external-logon-page MyExternalLogonPageAgent { uri "%{session.my_server_uri}" }**
  Creates the External Logon Page agent named **MyExternalLogonPageAgent** with a URI of **session.my_server_uri**.

- **list external-logon-page**
  Displays a list of External Logon Page agents.
- **delete external-logon-page MyExternalLogonPageAgent**
  Deletes the External Logon Page agent named **MyExternalLogonPageAgent**.

Options

- **[name]**
  Specifies the name of an External Logon Page agent. This option is required.
- **partition**
  Displays the partition within which the component resides.
- **app-service**
  Specifies the name of the application service to which the object belongs. The default value is **none**. **Note:** If the **strict-updates** option is **enabled** on the application service that owns the object, you cannot modify or delete the object. Only the application service can modify or delete the object.
- **split-username**
  Specifies whether user's input is split into username and domain. This option supports UPN style logon ID (userid@domainid) and Windows Domain User account ID (domainiduserid). The default is **false**. Set this to **true** when you want to store the username and domain separately.
- **uri**
  Specifies a predefined configuration that contains several settings that you want the agent to use to configure an External Logon page. This option is required.

See Also

logon-page

irule-event

Manages an iRule Event agent.

Syntax

Configure the **irule-event** component within the **policy agent** module using the syntax shown in the following sections.

Create/Modify

```
create irule-event [name]
modify irule-event [name]
    app-service [[string] | none]
    id [[string] | none]
edit irule-event  [ [ [name] | [glob] | [regex] ] ... ]
    all-properties
    non-default-properties
```

Display

```
list irule-event
list irule-event  [ [ [name] | [glob] | [regex] ] ... ]
show running-config irule-event
show running-config irule-event  [ [ [name] | [glob] | [regex] ] ... ]
    all-properties
    non-default-properties
    partition
show irule-event
show irule-event  [name]
```

Delete

```
delete irule-event  [name]
```

Description

You can use the **irule-event** component to add a custom Access iRule event to an access policy. This agent enables you to combine access policy execution with iRule execution.

For example, you can retrieve the current agent ID (using an iRule command ACCESS::policy agent_id) to determine which of the iRule agents raised the event and then perform some custom logic execution.

Examples

- **when ACCESS_POLICY_AGENT_EVENT {**
  if {[ACCESS::policy agent_id] eq "lastLogon" }
  $2weeks } { ACCESS::session data set

session.custom.lastLogonWithin2Weeks 0 } else { ACCESS::session data set session.custom.lastLogonWithin2Weeks 1 }
}
} >
In this example, ACCESS_POLICY_AGENT_EVENT gathers data containing the users whose last logon was within the last two weeks. Note that you can access session variables and create new session variables inside this event.

- **list irule-event all**
Displays a list of OAM agents.
- **delete irule-event my_irule_agent**
Deletes the iRule Event agent named **my_irule_agent**.

Options

- **app-service**
Specifies the name of the application service to which the object belongs. The default value is **none**. **Note:** If the **strict-updates** option is **enabled** on the application service that owns the object, you cannot modify or delete the object. Only the application service can modify or delete the object.
- **id**
Specifies the ID of the iRule event. The default is **none**. You can use the ID to determine which agent caused the ACCESS_POLICY_AGENT_EVENT. You can also use the ID to perform different processing inside iRule for different agents.
- **[name]**
Specifies the name of the component. This option is required.
- **partition**
Displays the partition within which the component resides.

kerberos

Manages a Kerberos agent.

Syntax

Configure the **kerberos** component within the **policy agent** module using the syntax shown in the following sections.

Create/Modify

```
create kerberos [name]
modify kerberos [name]
    app-service [[string] | none]
    max-logon-attempt [integer]
    server [string]
edit kerberos  [ [ [name] | [glob] | [regex] ] ... ]
    all-properties
    non-default-properties
```

Display

```
list kerberos
list kerberos [ [ [name] | [glob] | [regex] ] ... ]
show running-config kerberos
show running-config kerberos [ [ [name] | [glob] | [regex] ] ... ]
    all-properties
    non-default-properties
    partition
show kerberos
show kerberos [name]
```

Delete

```
delete kerberos [name]
```

Description

You can use the **kerberos** component to create and manage a Kerberos agent.

Examples

- **create kerberos my_kerberos_agent**
  Creates a Kerberos agent named **my_kerberos_agent**.
- **list kerberos all**
  Displays a list of Kerberos agents.

- **delete kerberos my_kerberos_agent**
  Deletes the Kerberos agent named **my_kerberos_agent**.

Options

- **[name]**
  Specifies the name of the component. This option is required.
- **app-service**
  Specifies the name of the application service to which the object belongs. The default value is **none**. **Note:** If the **strict-updates** option is **enabled** on the application service that owns the object, you cannot modify or delete the object. Only the application service can modify or delete the object.
- **max-logon-attempt**
  Specifies the maximum number of opportunities that users have to re-enter credentials after their first attempt to log in fails. If you set this value to a number from **2** to **5** inclusive, the system allows users the specified number of opportunities to log in after the first attempt to log in fails. If you set the value to **1**, the system does not allow a second log in opportunity after a first log in attempt fails. The default value is **3**.
- **partition**
  Displays the partition within which the component resides.
- **server**
  Specifies the name of the Kerberos server. This option is required.

logging

Manages a Logging agent.

Syntax

Configure the **logging** component within the **policy agent** module using the syntax shown in the following sections.

Create/Modify

```
create logging [name]
modify logging [name]
    app-service [[string] | none]
    log-message [[string] | none]
    variables [[string] | none]
edit logging [ [ [name] | [glob] | [regex] ] ... ]
    all-properties
    non-default-properties
```

Display

```
list logging
list logging [ [ [name] | [glob] | [regex] ] ... ]
show running-config logging
show running-config logging [ [ [name] | [glob] | [regex] ] ... ]
    all-properties
    app-service
    log-message
    non-default-properties
    partition
    variables
```

Delete

```
delete logging  [name]
```

Description

You can use the **logging** component to create and manage a logging agent that monitors the value of session variables and identifies the path taken by access policy execution. A logging agent can also be used to create and monitor custom or predefined session variables. Note that a session variable may or may not exist depending on the result of the access policy execution.

Examples

- **create logging MyProfile_act_logging_ag {**
  variables
  {

```
        {session-var "session.logon.*"}
        {session-var
"session.windows_check_file.Company8profile_act_file_check_ag.item_x.filename"}
      }
    }
```

Creates the logging agent named **MyProfile_act_logging_ag** in partition Common and adds two session variables
that define actions that the agent logs: **session.logon.*** indicates to log application logon attempts and
session.windows_check_file.Company8profile_act_file_check_ag.item_x.filename indicates to log the outcome
of the file check on the client. The x in item_x indicates the order of the files in the list configured for
the file checker. The list starts with index 0 (zero).

- **list logging**
  Displays a list of logging agents.

Options

- **app-service**
  Specifies the name of the application service to which the object belongs. The default value is **none**. **Note:** If the **strict-updates** option is **enabled** on the application service that owns the object, you cannot modify or delete the object. Only the application service can modify or delete the object.
- **log-message**
  Specifies the log message to display. This option is required.
- **[name]**
  Specifies the name of a logging agent. This option is required.
- **partition**
  Displays the partition within which the component resides.
- **variables**
  Adds a variable to or deletes a variable from a logging agent. You use the **sessionvar** option to specify a session variable that indicates what actions the system logs.

logon-page

Manages a Logon Page agent.

Syntax

Configure the **logon-page** component within the **policy agent** module using the following syntax.

Create/Modify

```
create logon-page [name]
modify logon-page [name]
    app-service [[string] | none]
    basic-auth-realm [[string] | none]
    customization-group [[string] | none]
    field-modifiable1 [true | false]
    field-modifiable2 [true | false]
    field-modifiable3 [true | false]
    field-modifiable4 [true | false]
    field-modifiable5 [true | false]
    field-type1 [checkbox | none | password | text]
    field-type2 [checkbox | none | password | text]
    field-type3 [checkbox | none | password | text]
    field-type4 [checkbox | none | password | text]
    field-type5 [checkbox | none | password | text]
    http-401-auth-level [basic | basic-negotiate | negotiate | none]
    post-var-name1 [[integer] | none]
    post-var-name2 [[integer] | none]
    post-var-name3 [[integer] | none]
    post-var-name4 [[integer] | none]
    post-var-name5 [[integer] | none]
    session-var-name1 [[integer] | none]
    session-var-name2 [[integer] | none]
    session-var-name3 [[integer] | none]
    session-var-name4 [[integer] | none]
    session-var-name5 [[integer] | none]
    split-username [true | false]
    type [401 | form-based]
edit logon-page [ [ [name] | [glob] | [regex] ] ... ]
    all-properties
    non-default-properties
```

Display

```
list logon-page
list logon-page [ [ [name] | [glob] | [regex] ] ... ]
show running-config logon-page
show running-config logon-page [ [ [name] | [glob] | [regex] ] ... ]
    all-properties
    non-default-properties
    partition
show logon-page
show logon-page [name]
```

Delete

```
delete logon-page [name]
```

Description

You can use the **logon-page** component to create and manage a Logon Page agent. This agent creates a logon page that includes the form in which users input the credentials required by an access policy. You can use the **customization-group** option to customize the logon page.

Examples

- **create logon-page MyLogonPageAgent my {**
  type 401
  basic-auth-realm myrealm
  split-username false
  http-401-auth-level none
  }
  Creates a basic authentication Logon Page agent named **MyLogonPageAgent** that results in a 401 response.
- **list logon-page**
  Displays a list of Logon Page agents.
- **delete logon-page MyLogonPageAgent**
  Deletes the Logon Page agent named **MyLogonPageAgent**.

Options

- **app-service**
  Specifies the name of the application service to which the object belongs. The default value is **none**. **Note:** If the **strict-updates** option is **enabled** on the application service that owns the object, you cannot modify or delete the object. Only the application service can modify or delete the object.
- **basic-auth-realm**
  Specifies the system being accessed for HTTP basic authentication. This value is shown in the 401 response. Use this option only for basic authentication Logon pages.
- **customization-group**
  Specifies a predefined configuration that contains several settings that you want the agent to use to configure a logon page. This setting is required, and the customization group that you assign must be of the type **logon**. Use this option only for basic authentication Logon pages.
- **field-modifiable1 - field-modifiable5**
  Specifies whether the user can modify the contents of the field on a form-based Logon page. The default is **true**. You can use this option to

display read-only information. A Logon page contains can have a maximum of five fields. Use this option only for form-based Logon pages.

- **field-type1 - field-type5**
  Specifies the type of fields on a form-based Logon page. The default is **text**. Use this option only for form-based Logon pages. The options are:
  - **checkbox**
  - **none**
  - **password**
  - **text**
- **http-401-auth-level**
  Use this option only for basic authentication Logon pages. The options are:
  - **basic**
  - **basic-negotiate**
  - **negotiate**
  - **none**
- **[name]**
  Specifies the name of a Logon Page agent. This setting is required.
- **partition**
  Displays the partition within which the component resides.
- **post-var-name1 - post-var-name5**
  Specifies the name of the variable that is sent with POST request. Use this option only for form-based Logon pages.
- **sess-var-name1 - sess-var-name5**
  Specifies the session variable from which the initial value is taken. Use this option only for form-based Logon pages.
- **split-username**
  Specifies whether the user's input is split into username and domain. This option supports UPN style logon ID (userid@domainid) and Windows Domain User account ID (domainiduserid). The default is **false**. Set this to true when you want to store the username and domain separately.
  Use this option only for basic authentication Logon pages.
- **type**
  Specifies the type of logon page that appears. The options are:
  - **401**
    Displays a basic HTTP authentication form.

- **form-based**
  Displays a logon page.

See Also

external-logon-page

message-box

Manages a Message Box agent.

Syntax

Configure the **message-box** component within the **policy agent** module using the syntax shown in the following sections.

Create/Modify

```
create message-box [name]
modify message-box [name]
    app-service [[string] | none]
    customization-group [string]
edit message-box [ [ [name] | [glob] | [regex] ] ... ]
    all-properties
    non-default-properties
```

Display

```
list message-box
list message-box [ [ [name] | [glob] | [regex] ] ... ]
show running-config message-box
show running-config message-box  [ [ [name] | [glob] | [regex] ] ... ]
    all-properties
    non-default-properties
    partition
show message-box
show message-box [name]
```

Delete

```
delete message-box [name]
```

Description

You can use the **message-box** agent to create, display, or delete a Message Box agent. You cannot use the command line interface to create or modify the messages that display in a message box. You can also edit customizable messages using the visual policy editor.

Examples

- **create message-box MyMessageBoxAgent { customization group "MyMessageBoxCG" }**
  Creates the Message Box agent named **MyMessageBoxAgent** that is associated with the
  customization group named **MyMessageBoxCG**.

- **list message-box**
  Displays a list of Message Box agents.
- **delete message-box MyMessageBoxAgent**
  Deletes the Message Box agent named **MyMessage BoxAgent**.

Options

- **[name]**
  Specifies the name of a Message Box agent. This option is required.
- **app-service**
  Specifies the name of the application service to which the object belongs. The default value is **none**. **Note:** If the **strict-updates** option is **enabled** on the application service that owns the object, you cannot modify or delete the object. Only the application service can modify or delete the object.
- **customization-group**
  Specifies the name of the customization group that contains the messages you want to apply to an access policy. This option is required.
- **partition**
  Displays the partition within which the component resides.

oam

Manages an OAM agent.

Syntax

Configure the **oam** component within the **policy agent** module using the syntax shown in the following sections.

Create/Modify

```
create oam [name]
modify oam [name]
    app-service [[string] | none]
    max-logon-attempt [integer]
    server [[string] | none]
    show-extended-error [true | false]
    url [[string] | none]
edit oam [ [ [name] | [glob] | [regex] ] ... ]
    all-properties
    non-default-properties
```

Display

```
list oam
list oam [ [ [name] | [glob] | [regex] ] ... ]
show running-config oam
show running-config oam  [ [ [name] | [glob] | [regex] ] ... ]
    all-properties
    non-default-properties
    partition
show oam
show oam [name]
```

Delete

```
delete oam [name]
```

Description

You can use the **oam** component to create and manage an OAM agent.

Examples

- **create oam oam_agent1 {**
  server oam10g
  max-logon-attempt 3
  show-extended-error false
  url "http://www.mydomain.com/protected/"

}

Creates an OAM agent named **oam_agent1** that uses authentication server **oam10g** and prompts a user for credentials three times before denying access to **http://www.mydomain.com/protected/**.

- **modify oam oam_agent1 max-logon-attempt 4**

- **list oam all**
  Displays a list of OAM agents.
- **delete oam my_oam_agent**
  Deletes the OAM agent named **my_tacacsplus_agent**.

Options

- **[name]**
  Specifies the name of the component. This option is required.
- **app-service**
  Specifies the name of the application service to which the object belongs. The default value is **none**. **Note:** If the **strict-updates** option is **enabled** on the application service that owns the object, you cannot modify or delete the object. Only the application service can modify or delete the object.
- **max-logon-attempt**
  Specifies the maximum number of opportunities that users have to re-enter credentials after their first attempt to log in fails. If you set this value to a number from **2** to **5** inclusive, the system allows users the specified number of opportunities to log in after the first attempt to log in fails. If you set the value to **1**, the system does not allow a second log in opportunity after a first log in attempt fails. The default value is **3**.
- **partition**
  Displays the partition within which the component resides.
- **server**
  Specifies the name of the OAM server used for user authentication. This option is required.
- **url**
  Specifies the URL of the resource that is protected by the OAM server. It is used to authenticate the user using the specified user credentials. This option is required, and you must specify an absolute URL. An absolute URL specifies the exact location of a file or directory on the Internet.
- **show-extended-error**
  Specifies to display a verbose error message on the retry logon page. The default value is **false**.

resource-assign

Manages a Resource Assign agent.

Syntax

Configure the **resource-assign** component within the **policy agent** module using the syntax shown in the following sections.

Create/Modify

```
create resource-assign [name]
modify resource-assign [name]
     app-service [[string] | none]
     rules (<string> | none)
     type [acls | general | resources | webtop-and-webtop-links]
edit resource-assign [ [ [name] | [glob] | [regex] ] ... ]
    all-properties
    non-default-properties
```

Display

```
list resource-assign
list resource-assign [ [ [name] | [glob] | [regex] ] ... ]
show running-config resource-assign
show running-config resource-assign  [ [ [name] | [glob] | [regex] ] ... ]
    all-properties
    non-default-properties
    partition
show resource-assign
show resource-assign [name]
```

Delete

```
delete resource-assign [name]
```

Description

You can use the **resource-assign** component to create and manage an agent that assigns an ACL, a resource group, or both to an access policy. A resource group is a collection of resources, access control lists, and protection criteria, which includes your company intranet servers, applications, and network shares. An ACL is a set of restrictions associated with a resource or favorite that defines access for users and groups.

Examples

- **create resource-assign MyAssignResourceAgent my rules {**
  { expression "expr { [mcget {session.ad.last.authresult}] == 1 }"
  webtop-links add { google }
  }
  }
  Creates the Resource Assign agent named **MyAssignResourceAgent** and assigns webtop-link **google** when authentication is passed.
- **list resource-assign all**
  Displays a list of Resource Assign agents.
- **delete resource-assign MyAssignResourceAgent**
  Deletes the Resource Assign agent named **MyAssignResourceAgent**.

Options

- **[name]**
  Specifies the name of the Resource Assign agent. This option is required.
- **partition**
  Displays the partition within which the component resides.
- **app-service**
  Specifies the name of the application service to which the object belongs. The default value is **none**. **Note:** If the **strict-updates** option is **enabled** on the application service that owns the object, you cannot modify or delete the object. Only the application service can modify or delete the object.
- **rules**
  Adds a rule to or deletes a rule from the Resource Assign agent. You can use the following attributes to define a rule:
  - **acl**
    Specifies an access control list that this rule assigns to users.
  - **connectivity-resource-group**
    Specifies the name of the connectivity resource group to which this rule applies.
  - **expression**
    Specifies the expression that indicates which resource groups this rule assigns to users.
- **type**
  Specifies the type of Resource Assign agent. The default is **general**.

route-domain-selection

Manages a Route Domain Selection agent.

Syntax

Configure the **route-domain-selection** component within the **policy agent** module using the syntax shown in the following sections.

Create/Modify

```
create route-domain-selection [name]
modify route-domain-selection [name]
    app-service [[string] | none]
    location-specific [true | false]
    route-domain [[integer] | none]
    snat [automap | none]
    snatpool [[string] | none]
edit route-domain-selection [ [ [name] | [glob] | [regex] ] ... ]
    all-properties
    non-default-properties
```

Display

```
list route-domain-selection
list route-domain-selection [ [ [name] | [glob] | [regex] ] ... ]
show running-config route-domain-selection
show running-config route-domain-selection  [ [ [name] | [glob] | [regex] ] ... ]
    all-properties
    non-default-properties
    partition
show route-domain-selection
show route-domain-selection [name]
```

Delete

```
delete route-domain-selection [name]
```

Description

You can use the **route-domain-selection** component to create a Route Domain Selection agent.

Examples

- **create route-domain-selection my_rds_ag route-domain 0 snat automap**
  Creates the **my_rds_ag** Route Domain Selection agent.

- **show route-domain-selection**
  Displays a list of Route Domain Selection agents.
- **delete route-domain-selection my_rd_selection_agent**
  Deletes the Route Domain Selection agent named **my_rd_selection_agent**.

Options

- **[name]**
  Specifies the name of a Variable Assignment agent. This option is required.
- **partition**
  Displays the partition within which the component resides.
- **app-service**
  Specifies the name of the application service to which the object belongs. The default value is **none**. **Note:** If the **strict-updates** option is **enabled** on the application service that owns the object, you cannot modify or delete the object. Only the application service can modify or delete the object.
- **location-specific**
  Specifies whether or not this object contains one or more attributes with values that are specific to the location where the BIG-IP device resides. The location-specific attribute is either true or false. When using policy sync, mark an object as location-specific to prevent errors that can occur when policies reference objects, such as authentication servers, that are specific to a certain location.
- **route-domain**
  Specifies the route domain. The default is **0** (zero).
- **snat**
  - **automap**
  - **none**
    Snat is not used.
- **snatpool**

tacacsplus

Manages a TACACS+ agent.

Syntax

Configure the **tacacsplus** component within the **policy agent** module using the syntax shown in the following sections.

Create/Modify

```
create tacacsplus
modify tacacsplus
    app-service [[string] | none]
    max-logon-attempt [integer]
    server [[string] | none]
edit tacacsplus [ [ [name] | [glob] | [regex] ] ... ]
    all-properties
    non-default-properties
```

Display

```
list tacacsplus
list tacacsplus [ [ [name] | [glob] | [regex] ] ... ]
show running-config tacacsplus
show running-config tacacsplus [ [ [name] | [glob] | [regex] ] ... ]
    all-properties
    non-default-properties
    partition
show tacacsplus
show tacacsplus [name]
```

Delete

```
delete tacacsplus [name]
```

Description

You can use the **tacacsplus** component to create and manage a TACACS+ agent.

Examples

- **list tacacsplus all**
  Displays a list of TACACS+ agents.
- **delete tacacsplus my_tacacsplus_agent**
  Deletes the TACACS+ agent named **my_tacacsplus_agent**.

Options

- **[name]**
  Specifies the name of the component. This option is required.
- **app-service**
  Specifies the name of the application service to which the object belongs. The default value is **none**. **Note:** If the **strict-updates** option is **enabled** on the application service that owns the object, you cannot modify or delete the object. Only the application service can modify or delete the object.
- **max-logon-attempt**
  Specifies the maximum number of opportunities that users have to re-enter credentials after their first attempt to log in fails. If you set this value to a number from **2** to **5** inclusive, the system allows users the specified number of opportunities to log in after the first attempt to log in fails. If you set the value to **1**, the system does not allow a second log in opportunity after a first log in attempt fails. The default value is **3**.
- **partition**
  Displays the partition within which the component resides.
- **server**
  Specifies the name of the TACACS+ server. This option is required.

variable-assign

Manages a Variable Assignment agent.

Syntax

Configure the **variable-assign** component within the **policy agent** module using the syntax shown in the following sections.

Create/Modify

```
create variable-assign [name]
modify variable-assign [name]
    app-service [[string] | none]
    type [citrix-smart-access | general | intranet-webtop | sso-cred-mapping |
virtual-keyboard]
    variables { [varname [name] expression {[string] }}
edit variable-assign [ [ [name] | [glob] | [regex] ] ... ]
    all-properties
    non-default-properties
```

Display

```
list variable-assign
list variable-assign [ [ [name] | [glob] | [regex] ] ... ]
show running-config variable-assign
show running-config variable-assign  [ [ [name] | [glob] | [regex] ] ... ]
    all-properties
    non-default-properties
    partition
show variable-assign
show variable-assign [name]
```

Delete

```
delete variable-assign [name]
```

Description

You can use the **variable-assign** component to create and manage an agent that assigns one or more variables to an access policy. F5 Networks recommends that you use the visual policy editor to create complex variable assignments.

Examples

- **create variable-assign username_variable_assign_ag {**
  variables
  { varname "session.logon.last.username" expression "{[mcget

{session.ssl.cert.cn}]}" }
}
Creates the **username_variable_assign_ag** Variable Assignment agent that automatically
assigns the value of the common name field in the client certificate to the username field of
the logon page. This is useful when an access policy contains the Variable Assignment agent
between the client certification and the AAA Active Directory server query actions.

- **create variable-assign acl_variable_assign_ag {**
variables
{ varname
"config.connectivity_resource_network_access.MyprofileNR2.acl_name"
expression "expr {"MY_ACL1"}"
}
}
Creates a Variable Assignment agent that carries out a configured ACL when a particular branch in the access
policy is followed, using the Variable Assignment agent to populate the appropriate variables with
the ACL name.
- **show variable-assign**
Displays a list of Variable Assignment agents.
- **delete variable-assign MyAssignVariableAgent delete**
Deletes the Variable Assignment agent named **MyAssignVariableAgent**.

Options

- **[name]**
Specifies the name of a Variable Assignment agent. This setting is required.
- **partition**
Displays the partition within which the component resides.
- **app-service**
Specifies the name of the application service to which the object belongs. The default value is **none**. **Note:** If the **strict-updates** option is **enabled** on the application service that owns the object, you cannot modify or delete the object. Only the application service can modify or delete the object.
- **type**
Specifies the type of agent. The default is general.
- **variables**
Adds a variable to or deletes a variable from the Variable Assignment agent. You must specify the following attributes for each variable:

- **expression**
  A Tcl expression that the system evaluates, and then assigns the value of the expression to a specific property of the assigned Network Access resource or to a newly created session variable.
- **varname**
  A variable that forms the left-hand side of the expression. You can use the name of an existing variable or a new session variable.

36

apm profile

- Introducing the apm profile module
- Alphabetical list of components

Introducing the apm profile module

You can use the tmsh components that reside within the apm profile module to configure BIG-IP® Access Policy Manager®. For more information about the tmsh hierarchical structure, see Chapter 2, *Understanding and Using the Traffic Management Shell*.

Alphabetical list of components

The remainder of this chapter lists the tmsh components that are available in the apm profile module.

access

Configures an access profile.

Syntax

Configure the **access** component within the **profile** module using the syntax shown in the following sections.

Create/Modify

```
create access [name]
modify access [name]
    accept-languages [add | delete | modify | replace-all-with] {
      [name]
    }
    access-policy [[string] | none]
    access-policy-timeout [integer]
    app-service [[string] | none]
    cache-generation [integer]
    customization-group [[string] | none]
    default-language [[string] | none]
    defaults-from [[string] | none]
    domain-cookie [[string] | none]
    domain-groups [add | delete | modify | replace-all-with] {
      [name]
    }
    domain-mode [single-domain | multi-domain]
    user-identity-method [http | ip-address]
    eps-group [[string] | none]
    errormap-group [[string] | none]
    framework-installation-group [[string] | none]
    general-ui-group [[string] | none]
    generation-action [increment | noop]
    httponly-cookie [true | false]
    inactivity-timeout [integer]
    logout-uri-include [add | delete | modify | replace-all-with] {
      [name]
    }
    logout-uri-timeout [integer]
    log-settings [add | delete | modify | replace-all-with] {
       [name]
    }
    max-concurrent-sessions [[integer] | none]
    max-concurrent-users [[integer] | none]
    max-failure-delay [integer]
    max-in-progress-sessions [[integer] | none]
    max-session-timeout [integer]
    min-failure-delay [integer]
    persistent-cookie [true | false]
    primary-auth-service [[string] | none]
    restrict-to-single-client-ip [true | false]
    sandboxes [add | delete | modify | replace-all-with] {
      [name] { retain-public-access [true|false] }
    }
    secure-cookie [true | false]
    sso-name [[string] | none]
```

```
edit access [ [ [name] | [glob] | [regex] ] ... ]
    all-properties
    non-default-properties
```

Display

```
list access
list access [ [ [name] | [glob] | [regex] ] ... ]
show running-config access
show running-config access [ [ [name] | [glob] | [regex] ] ... ]
    all-properties
    non-default-properties
    partition
show access
show access [name]
```

Delete

```
delete access [name]
```

Description

You can use the **access** component to configure an access profile. An access profile is a pre-configured group of settings that you can use to configure secure Network Access for an application.

Examples

- **create access MyAccessProfile {**
  defaults-from access
  access-policy "my_access_policy"
  accepted-languages "my_accepted_languages"
  default-language "en"
  customization-group "company_logout"
  eps-group 'myepsgroup'
  framework-installation-group "company_header"
  "company_footer"
  errormap-group "company_errormap"
  }

  Creates an access profile named **MyAccessProfile** that is based on the default access profile named **access**, uses the access policy named **my_access-policy**, accepts the languages in the **my_accepted_languages** class, uses English as the default language, and uses these groups to customize the application pages and messages: company_logout, company_header, company_footer, and company_errormap.
- **list access all all-properties**
  Displays a list of access profiles, including parameter values.
- **delete access MyAccessProfile**
  Deletes the access profile named **MyAccessProfile**.

Options

- **accept-languages**
  Specifies the name of a class that defines the languages supported by the access profile. The default languages are en (English), ja (Japanese), zh-cn (simplified Chinese (PRC)), and zh tw (traditional Chinese (Taiwan)). This option is required.
- **access-policy**
  Specifies the access policy that you want to enforce using this access profile. An access policy contains various security checks that a client must pass before the BIG-IP Access Policy Manager grants access to a protected application. This option is required.
- **access-policy-timeout**
  Specifies, for this access profile, the number of seconds within which a user must complete the steps to gain access to an application. The default is **300** seconds. This option is designed to quickly release session resources when a user does not complete the access process, for example, when the user closes the browser before completing the access process.
- **app-service**
  Specifies the name of the application service to which the object belongs. The default value is **none**. **Note:** If the **strict-updates** option is **enabled** on the application service that owns the object, you cannot modify or delete the object. Only the application service can modify or delete the object.
- **customization-group**
  Specifies the customization group that defines the appearance of the logout and error pages. This option is required.
- **default-language**
  Specifies the default language for the BIG-IP Access Policy Manager that you want to implement with this access profile. The default is **en** (English). If the client requests a language that is not supported, the BIG-IP Access Policy Manager uses the default value. This option is required.
- **defaults-from**
  Specifies the default access policy from which this profile is created. This option is required.
- **domain-cookie**
  Specifies a domain cookie to use with an application access control connection. If you specify a domain cookie, then the line **domain=specified_domain** is added to the MRHsession cookie. The default is **none**.
- **domain-groups**
  Specifies a group of multiple domains or multiple hosts in multiple domains to which a single user session has access. For example, you can use this option to configure a single user session to have access to three domains: www.a.com, www.b.com, and www.c.com. When a user logs in to any of these domains, that user can access the other domains without logging in again. This option is required when you set the

domain-mode option to **multi-domain**.
For each domain in the domain group, you can specify the following settings:

- **cookie-host**
  Specifies the host name for which to create the user's session cookie.
- **cookie-domain**
  Specifies the domain for which to create the user's session cookie.
- **secure-cookie**
  Adds a security attribute to the user's session cookie.
- **persistent-cookie**
  Adds a persistence attribute to the user's session.
- **sso-name**
  Specifies the SSO method to use when accessing a backend application.

◆ **domain-mode**
Specifies how the SSO configuration is applied. The options are:

- **single-domain**
  Applies the SSO configuration to a single domain. This is the default. When you set **domain-mode** to **single-domain**, you must also set the **sso-name** option.
- **multi-domain**
  Applies the SSO configuration across multiple domains. This option allows users a single APM login/session and applies the credentials across multiple Local Traffic Manager or Access Policy Manager virtual servers in front of different domains. Note that to apply SSO configurations across multiple domains, all virtual servers must be on one BIG-IP system.
  When you set **domain-mode** to **multi-domain**, you must also configure the **domain-group** option, and provide a URI for the **primary-auth-service** option.

◆ **user-identity-method**
Specifies how access will bind a session to a request.

- **http**
  Use http information such as cookies and URI query string to identify user.
- **ip-address**
  Use IP address to identify a user. Do not use this setting if clients may be behind a NAT.

◆ **eps-group**
This option is required.

◆ **errormap-group**
Specifies the customization settings for the error map that you want to implement with this access profile. This setting is required.

◆ **framework-installation-group**
Specifies the customization settings for the header and footer that you want to implement with this access profile. This setting is required.

- **generation-ui-group**
  Specifies the generation of the user interface group for the new generation access configuration. This option is required.
- **generation-timeout**
  Specifies the timeout, in seconds, for the new generation access configuration.
- **generation-action**

  - **increment**
    Activates the current access policy configuration for an access profile. For example, the following command activates current access policy configuration for profile myAccessProfile: tmsh modify apm profile access myAccessProfile generation-action increment
  - **noop**
    Specifies "no operation to be performed". This is the default.
  - **sync**
    Specifies that the policy is being modified due to APM policy sync operation. This is an internal action; you should not set it.
- **httponly-cookie**
  Specifies whether HttpOnly directive should be inserted in HTTP response from BIG-IP. The client browser should prevent script from accessing cookie, if this flag is set in the response. The default is **false**.
- **inactivity-timeout**
  Specifies, for this access profile, the number of seconds that the session on the client can be idle before the server disconnects the VPN tunnel. The default is **900** seconds.
- **logout-uri-include**
  Specifies a list of URIs to include in the access profile for initiating session logout.
- **logout-uri-timeout**
  Specifies the timeout used to delay logout for the customized logout URIs defined in the logout uri include list
- **log-settings**
  Specifies one or more log-setting containers to associate with this profile
- **max-concurrent-sessions**
  Specifies, for this access profile, the number of concurrent sessions allowed. The default is **0** (zero), which represents unlimited sessions. Users assigned an administrative role of **Application Editor** can view the value of this option. Users assigned any other administrative role can modify this option.
- **max-concurrent-users**
  Specifies, for this access profile, the number of concurrent sessions allowed. The default is 0 (zero), which represents unlimited sessions. This field is Read-only for Application Editors. Users assigned any other administrative role can modify this field.

- **max-failure-delay**
  Specifies the maximum random delay after authentication failure during the access policy. It is the maximum number of seconds before the user is shown an error message on the logon page and prompted to re-enter credentials. The default is **5** seconds. **0** (zero) represents no delay. Note: Set max-failure-delay to no more than one-half the access-policy-timeout value and no more than 65 seconds greater than min-failure-delay.
- **max-in-progress-sessions**
  Specifies the maximum number of in-progress concurrent sessions a user can have. The in-progress sessions are the sessions for which an access policy has not completed. The default is **0**, which represents an unlimited number of such sessions.
- **max-session-timeout**
  Specifies the maximum lifetime of one session. The maximum lifetime is the number of seconds between session creation and session termination.
- **min-failure-delay**
  Specifies the minimum random delay after authentication failure during the access policy. It is the minimum number of seconds before the user is prompted for credentials again or shown an error message on the logon page. The default is **2** seconds.
- **[name]**
  Specifies the name of the access profile. This option is required.
- **persistent-cookie**
  Specifies to retain the cookie for a user session, even when the user session is terminated, when set to **true**. Although this is an insecure method, this setting is useful and required in cases where you have a third-party application, such as Sharepoint, and need to store the cookie in a local database so that any attempt to access backend server applications through Access Policy Manager succeeds. The default is **false**.
- **primary-auth-service**
  Specifies the address of your primary authentication URI. This setting is required when you set the **domain-mode** option to **multi-domain**.
  For example, when you set this option to **https://logon.yourcompany.com**, the user session is stored on this primary domain, and the user can access multiple backend applications from multiple domains and hosts without re-entering credentials.
- **restrict-to-single-client-ip**
  Specifies whether a user session is tied to a single client IP. If during session's lifetime, the user's client IP address changes, the current session is terminated. The user needs to re-login to create a new session from the new client IP address. The default is **false**.
- **sandboxes**
  Specifies the association between the access profile and the sandbox. If **retain-public-access** is set to true, this association is retained even if there is no resource that uses sandbox files in the access policy that corresponds to this access profile.

- **secure-cookie**
  Set this option to **true**, if you want to add a secure keyword to the session cookie. Set this option to **false**, if you want to configure an application access control scenario that uses an HTTPS virtual server to authenticate the user, and then sends the user to an existing HTTP virtual server to use applications. The default is **true**.
- **sso-name**
  Specifies the SSO configuration that you want BIG-IP Access Policy Manager to use to submit the user's credentials to the backend application. This allows the user to log in once to the Access Policy Manager and then gain access to backend applications without logging in again.

See Also

apm sso, *apm policy*

connectivity

Configures a connectivity profile.

Syntax

Configure the **connectivity** component within the **profile** module using the syntax shown in the following sections.

Create/Modify

```
create connectivity [name]
modify connectivity [name]
     adaptive-compression [enabled | disabled]
     app-service [[string] | none]
     citrix-client-bundle [[name] | default-citrix-client-bundle]
     component-update [yes | prompt | no]
     compress-buffer-size [integer]
     compress-cpu-saver [true | false]
     compress-cpu-saver-high [integer]
     compress-cpu-saver-low [integer]
     compress-gzip-level [integer]
     compress-gzip-memlevel [integer]
     compress-gzip-window-size [integer]
     compress-ingress [true | false]
     compress-preferred-method [[string] | none]
     compression [enabled | disabled]
     compression-codecs [[string] | none]
     customization-group [[string] | none]
     defaults from [[name] | none]
     deflate-compression-level [integer]
     enforce-session-settings [true | false]
     location-dns [[string] | none]
     location-specific [true | false]
     reuse-winlogon-creds [true | false]
     save-password [true | false]
     save-password-method [disk | memory]
     save-password-timeout [integer]
     save-servers-on-exit [true | false]
     servers [add | delete | modify | replace-all-with] {
      [name]
     }
     tunnel-name [[string] | none]
     win-mobile-server [[string] | none]
     win-mobile-work-url-exceptions [[string] | none] [add | delete | modify |
replace-all-with] {
      [name]
     }
edit connectivity [ [ [name] | [glob] | [regex] ] ... ]
    all-properties
    non-default-properties
```

Display

```
list connectivity
list connectivity [ [ [name] | [glob] | [regex] ] ... ]
show running-config connectivity
show running-config connectivity [ [ [name] | [glob] | [regex] ] ... ]
    all-properties
    non-default-properties
    partition
show connectivity
show connectivity [name]
```

Delete

```
delete connectivity [name]
```

Description

You can use the **connectivity** component to configure a connectivity profile. By using the connectivity profile, you can configure L2 and L4 tunnels, compression, Windows and mobile client settings, and client component downloads from F5 Networks and Citrix.

Examples

create connectivity myconnectivityprofile { }

Creates a connectivity profile named **myconnectivityprofile** that inherits its settings from the system default connectivity profile.

Options

- **adaptive-compression**
  Enables or disables adaptive compression. Use this option to configure compression settings for application tunnels and to optimize applications and RDP traffic. The default is **enabled**.
- **app-service**
  Specifies the name of the application service to which the object belongs. The default value is **none**. **Note:** If the **strict-updates** option is **enabled** on the application service that owns the object, you cannot modify or delete the object. Only the application service can modify or delete the object.
- **citrix-client-bundle**
  Specifies the Citrix client bundle used by this connectivity profile. The default is **default-citrix-client-bundle**.
- **component-update**
  Specifies how the Secure Access Client handles automatic updates. The options are:

- **yes**
  Automatically installs a client update when one is available.
- **prompt**
  Prompts the user about installing a client update.
- **No**
  Disables the client from receiving automatic updates.

- **compress-buffer-size**
  Specifies the size of compressed data for Network Access tunnels. The default is **4096**.
- **compress-cpu-saver**
  Specifies whether the system monitors the percentage of CPU usage and adjusts compression rates automatically when CPU usage reaches either the CPU saver high threshold or the CPU saver low threshold. The default is **true**.
- **compress-cpu-saver-high**
  Specifies the percentage of CPU usage at which the system starts automatically decreasing the amount of content being compressed, as well as the amount of compression which the system is applying. The default is **90** percent.
- **compress-cpu-saver-low**
  Specifies the percentage of CPU usage at which the system resumes content compression at the user-defined rates. The default is **75** percent.
- **compress-gzip-level**
  Specifies the degree to which the system compresses the content. Higher compression levels slow down the compression process. The default is **6**, which provides a higher amount of compression at the expense of more CPU processing time. **1** is the lowest level and **9** is the highest level. **0** disables compression.
- **compress-gzip-memlevel**
  Specifies the number of kilobytes of memory that the system uses for internal compression buffers when compressing data. You can select a value between 1 and 256. The default is **8192**.
- **compress-gzip-window-size**
  Specifies the number of kilobytes in the window size that the system uses when compressing data. You can select a value between 1 and 128. The default is **16384**.
- **compress-ingress**
  Specifies whether incoming data is compressed. The default is **false**.
- **compress-preferred-method**
  Specifies the preferred method of data compression. The default is **zlib**.
- **compression**
  Enables or disables compression between the client and the server. The default is **enabled**.
- **compression-codecs**
  Specifies the available compression codecs for server-to-client connections. The server compares the available compression types you configure with the available compression types on the client, and then

chooses the most effective mutual compression setting. Compression for the client is configured separately. The default includes all three available codecs:

- **lzo**
  Offers a balance between CPU resources and compression ratio, compressing more than **deflate**, but with less CPU resources than **bzip2**.
- **deflate**
  Uses the least CPU resources, but compresses the least effectively.
- **bzip2**
  Uses the most CPU resources, but compresses the most effectively.

◆ **customization-group**
Specifies which customization groups are applied. This option is required.

◆ **defaults-from**
Specifies the profile from which this profile inherits properties that are not specified explicitly. The default is **connectivity**.

◆ **deflate-compression-level**
Specifies the level of compression performed by the **deflate** codec. The default is **1**.

◆ **enforce-session-settings**
Specifies whether Secure Access Client always honors the session settings configured by the administrator on the server, or can use settings selected by the user. The default is **false**. The options are:

- **false**
  Ensures that the Secure Access Client always uses the session settings configured on the server.
- **true**
  Ensures that the Secure Access Client uses settings chosen by the user.

◆ **location-dns**
Specifies a list of DNS suffixes used by the Network Location Awareness feature of the Secure Access Client. This list represents the internal network where local resources are available without the need of a Network Access connection. The default is **none**.

◆ **location-specific**
Specifies whether or not this object contains one or more attributes with values that are specific to the location where the BIG-IP device resides. The location-specific attribute is either true or false. When using policy sync, mark an object as location-specific to prevent errors that can occur when policies reference objects, such as authentication servers, that are specific to a certain location.

◆ **[name]**
Specifies the profile that you want to use as the parent profile. The new profile inherits all settings and values from the parent profile.

- **reuse-winlogon-creds**
  Specifies whether Secure Access Client can reuse logon credentials entered by a user for a subsequent log in. The default is **false**.
- **save-password**
  Specifies whether Secure Access Client allows user password caching. The default is **true**.
- **save-password-method**
  Specifies whether Secure Access Client saves encrypted passwords on disk or caches passwords in memory only. The default is **disk**.
- **save-password-timeout**
  Specifies the number of minutes that a cached password remains valid (applies only to in-memory password caching). The default is **240**.
- **save-servers-on-exit**
  Specifies whether Secure Access Client maintains a list of Access Policy Manager systems that the client accessed. The default is **true**.
- **servers**
  Specifies a list of server and alias pairs in the Secure Access Client's server list. Delimit server and alias entries using double colons ("::"). For example, **"server1::alias2"**.
- **tunnel-name**
  Specifies the name of the tunnel through which data passes. The default is **none**.
- **win-mobile-server**
  Specifies a server URL to which Secure Access Client for Windows Mobile can connect. The default is **none**.
- **win-mobile-work-url-exceptions**
  Specifies IP addresses and domain names that can be accessed through Secure Access Client, for example **192.168.*, *.company.com, server.company.com**. The default is **none**.

See Also

apm profile, *virtual*

exchange

Configures an exchange profile.

Syntax

Configure the **exchange** component within the **profile** module using the syntax shown in the following sections.

Create/Modify

```
create exchange [name]
modify exchange [name]
    ntlm-auth-name [[string] | none]
    active-sync-url [[string] | none]
    active-sync-auth-type [basic | ntlm | basic-ntlm]
    active-sync-sso-config [[string] | none]
    auto-discover-url [[string] | none]
    auto-discover-auth-type [basic | ntlm | basic-ntlm]
    auto-discover-sso-config [[string] | none]
    offline-address-book-url [[string] | none]
    offline-address-book-auth-type [basic | ntlm | basic-ntlm]
    offline-address-book-sso-config [[string] | none]
    rpc-over-http-url [[string] | none]
    rpc-over-http-auth-type [basic | ntlm | basic-ntlm]
    rpc-over-http-sso-config [[string] | none]
    user-agent-pattern-for-utf8 [[string] | none]
    web-service-url [[string] | none]
    web-service-auth-type [basic | ntlm | basic-ntlm]
    web-service-sso-config [[string] | none]
edit exchange [ [ [name] | [glob] | [regex] ] ... ]
    all-properties
    non-default-properties
```

Display

```
list exchange
list exchange [ [ [name] | [glob] | [regex] ] ... ]
show running-config exchange
show running-config exchange [ [ [name] | [glob] | [regex] ] ... ]
    all-properties
    non-default-properties
    partition
show exchange
show exchange [name]
```

Delete

```
delete exchange [name]
```

Description

You can use the **exchange** component to configure an exchange profile. An exchange profile is a preconfigured group of settings that you can use to configure authentication for exchange services such as Outlook Anywhere, ActiveSync, Autodiscover and Offline Address Book, so that those work with BIG-IP.

Examples

```
create exchange  MyExchangeProfile {
  ntlm-auth-name "MyNTLMAuth"
  rpc-over-http-url "/rpc/rpcproxy.dll"
  rpc-over-http-auth-type  ntlm
  rpc-over-http-sso-config "MyKerberosSSOConfig"
}>
```

Creates an exchange profile named **MyExchangeProfile** that is based on the general settings such as NTLM Authentication configuration **MyNTLMAuth**. The profile is configured for Outlook Anywhere (RPC over HTTP) service with url **"/rpc/rpcproxy.dll***, client authentication type **ntlm** and SSO configuration
type **MyKerberosSSOConfig**

- **list exchange all all-properties**
  Displays a list of exchange profiles, including parameter values.
- **delete access MyExchangeProfile**
  Deletes the exchange profile named **MyExchangeProfile**.

Options

- **ntlm-auth-name**
  Specifies the NTLM configuration object that clients can use to authenticate on the front-end. Backend SSO type must be Kerberos for ntlm or basic-ntlm front end.
- **active-sync-auth-type**
  Specifies the client-side authentication type for ActiveSync exchange service. The valid value is basic.
- **active-sync-sso-config**
  Specifies the back end SSO config for ActiveSync exchange service. This is optional.
- **active-sync-url**
  Specifies the URL for ActiveSync exchange service. URL is required for ActiveSync service to be enabled through BIG-IP.
- **auto-discover-auth-type**
  Specifies the client-side authentication type for Autodiscover exchange service. The valid values are basic, ntlm and basic-ntlm.

- **auto-discover-sso-config**
  Specifies the back end SSO config for Autodiscover exchange service. This is optional.
- **auto-discover-url**
  Specifies the URL for Autodiscover exchange service. URL is required for Autodiscover service to be enabled through BIG-IP.
- **offline-address-book-auth-type**
  Specifies the client-side authentication type for Offline Address Book exchange service. The valid values are basic, ntlm and basic-ntlm.
- **offline-address-book-sso-config**
  Specifies the back end SSO config for Offline Address Book exchange service. This is optional.
- **offline-address-book-url**
  Specifies the URL for Offline Address Book exchange service. URL is required for Offline Address Book service to be enabled through BIG-IP.
- **rpc-over-http-auth-type**
  Specifies the client-side authentication type for Outlook Anywhere (RPC over HTTP) exchange service. The valid values are basic, ntlm and basic-ntlm.
- **rpc-over-http-sso-config**
  Specifies the back end SSO config for Outlook Anywhere (RPC over HTTP) exchange service. This is optional.
- **rpc-over-http-url**
  Specifies the URL for Outlook Anywhere (RPC over HTTP) exchange service. URL is required for Outlook Anywhere (RPC over HTTP) service to be enabled through BIG-IP.
- **user-agent-pattern-for-utf8**
  Specifies the user agent pattern for UTF8.
- **web-service-auth-type**
  Specifies the client-side authentication type for Web Exchange service. The valid values are basic, ntlm and basic-ntlm.
- **web-service-sso-config**
  Specifies the back end SSO config for Web Exchange service. This is optional.
- **web-service-sync-url**
  Specifies the URL for Web Exchange service. URL is required for Web Service to be enabled through BIG-IP.

See Also

apm sso, *access*

remote-desktop

Displays information about a default profile that supports a Citrix remote desktop resource.

Syntax

Displays the properties of the **remote-desktop** component within the **profile** module.

Display

```
list remote-desktop
list remote-desktop [ [ [name] | [glob] | [regex] ] ... ]
show running-config remote-desktop
show running-config remote-desktop [ [glob] | [regex] ] ... ]
    all-properties
    location-specific [true | false]
    non-default-properties
    one-line
```

Description

You can use the **remote-desktop** component to display the properties of the default remote desktop profile.

A remote desktop profile is for internal use only. You should not create or modify a remote desktop profile.

Examples

list remotedesktop all-properties

Displays all of the properties of the default remote desktop profile.

- **location-specific**
  Specifies whether or not this object contains one or more attributes with values that are specific to the location where the BIG-IP device resides. The location-specific attribute is either true or false. When using policy sync, mark an object as location-specific to prevent errors that can occur when policies reference objects, such as authentication servers, that are specific to a certain location.

See Also

virtual

vdi

Configures a VDI profile.

Syntax

Configure the **vdi** component within the **profile** module using the syntax shown in the following sections.

Create/Modify

```
create vdi [name]
modify vdi [name]
    msrdp-ntlm-auth-name [[string] | none]
edit vdi [ [ [name] | [glob] | [regex] ] ... ]
    all-properties
    non-default-properties
```

Display

```
list vdi
list vdi [ [ [name] | [glob] | [regex] ] ... ]
show running-config vdi
show running-config vdi [ [glob] | [regex] ] ... ]
    all-properties
    non-default-properties
    one-line
```

Delete

```
delete vdi [name]
```

Description

You can use the **vdi** component to configure a VDI profile. A VDI profile is a group of settings that you can use to enable and configure VDI services such as Citrix, VMware View and MSRDP, so that those work with the BIG-IP system.

Examples

```
create vdi MyVdiProfile {
  msrdp-ntlm-auth-name "MyNTLMAuth"
}
```

Creates a VDI profile named **MyVdiProfile** with NTLM Authentication configuration **MyNTLMAuth** to be used for MSRDP clients authentication.

- **list vdi all-properties**
  Displays a list of VDI profiles, including parameter values.

- **delete vdi MyVdiProfile**
  Deletes the VDI profile named **MyVdiProfile**.

Options

- **msrdp-ntlm-auth-name**
  Specifies the NTLM auth configuration object to be used by this VDI profile for MSRDP client authentication.

See Also

virtual

37

apm resource

- Introducing the apm resource module
- Alphabetical list of components

Introducing the apm resource module

You can use the tmsh components that reside within the apm resource module to configure BIG-IP® Access Policy Manager®. For more information about the tmsh hierarchical structure, see Chapter 2, *Understanding and Using the Traffic Management Shell*.

Alphabetical list of components

The remainder of this chapter lists the tmsh components that are available in the apm resource module.

app-tunnel

Configures an application tunnel.

Syntax

Configure the **app-tunnel** component within the **resource** module using the syntax shown in the following sections.

Create/Modify

```
create app-tunnel [name]
modify app-tunnel [name]
    acl-order [integer]
    app-service [[string] | none]
    application-launch-warning [true | false]
    apps [add | delete | modify | replace-all-with] {
      [name]
    }
    customization-group [add | delete | modify | replace-all-with] {
      [name]
    }
    description [[string] | none]
    location-specific [true | false]
    type [app-tunnel | last | network-access | remote-desktop | web-application]
edit app-tunnel [ [ [name] | [glob] | [regex] ] ... ]
    all-properties
    non-default-properties
```

Display

```
list app-tunnel
list app-tunnel [ [ [name] | [glob] | [regex] ] ... ]
show running-config app-tunnel
show running-config app-tunnel [ [ [name] | [glob] | [regex] ] ... ]
    all-properties
    non-default-properties
    one-line
show app-tunnel
show app-tunnel [name]
```

Delete

```
delete app-tunnel [name]
```

Description

You can use the **app-tunnel** component to configure an application tunnel to provide secure access to a network, remote desktop, or specific applications.

Examples

item **create app-tunnel myapptunnel customization-group myapptunnelcg**

Creates an application tunnel named **myapptunnel** that uses the policies in the customization group **myapptunnelcg**.

item **delete app-tunnel myapptunnel**

Deletes the application tunnel named **myapptunnel**.

Options

- **acl-order**
  Specifies the location of this app tunnel in the ACL heirarchy in Access Policy Manager ACL lists. The default is **0** (zero).
- **app-service**
  Specifies the name of the application service to which the object belongs. The default value is **none**. **Note:** If the **strict-updates** option is **enabled** on the application service that owns the object, you cannot modify or delete the object. Only the application service can modify or delete the object.
- **application-launch-warning**
  Specifies whether to display a warning before launching an application. The options are:
  - **true**
    The system displays security warnings before launching an application, regardless of whether the site is considered a Trusted site. This is the default value.
  - **false**
    The system displays security warnings before launching an application, only if the site is not in the Trusted Sites list.
- **apps**
  Specifies the applications that a user can access using this application tunnel. The default is **none**.
- **customization-group**
  Specifies whether customizations are applied to the application tunnel. You can add, modify, delete, or replace all customization groups. This option is required.
- **description**
  Specifies a description for the application tunnel. The default is **none**.
- **location-specific**
  Specifies whether or not this object contains one or more attributes with values that are specific to the location where the BIG-IP device resides. The location-specific attribute is either true or false. When using policy sync, mark an object as location-specific to prevent errors that can occur when policies reference objects, such as authentication servers, that are specific to a certain location.

- **[name]**
  Specifies a name for the component.
- **partition**
  Displays the partition within which the **app-tunnel** component resides. The default is **common**.
- **type**
  Specifies the type of application tunnel. The options are:
  - **app-tunnel**
    This is the default.
  - **network-access**
    Provides access to a network.
  - **remote-desktop**
    Provides access to a remote desktop.
  - **web-application**
    Provides access to a Web application.

client-rate-class

Configures a client rate class resource.

Syntax

Configure the **client-rate-class** component within the **resource** module using the syntax shown in the following sections.

Create/Modify

```
create client-rate-class [name]
modify client-rate-class [name]
    app-service [[string] | none]
    burst [integer]
    ceiling [integer]
    description [[string] | none]
    dscp [integer]
    location-specific [true | false]
    mode [borrow | discard | shape]
    rate [integer]
    type [best-effort | controlled-load | guaranteed]
edit client-rate-class [ [ [name] | [glob] | [regex] ] ... ]
    all-properties
    non-default-properties
```

Display

```
list client-rate-class
list client-rate-class [ [ [name] | [glob] | [regex] ] ... ]
show running-config client-rate-class
show running-config client-rate-class [ [ [name] | [glob] | [regex] ] ... ]
    all-properties
    non-default-properties
show client-rate-class
show client-rate-class [name]
```

Delete

```
delete client-rate-class [name]
```

Description

You can use the **client-rate-class** component to configure a client rate class resource, which is used in traffic control.

Examples

- **create client-rate-class sf1{**
  dscp 40
  rate 60000
  ceiling 80000
  mode shape
  }
  Creates a client rate class resource named **sf1** used in traffic control. Sets the dscp
  to **40** and the rate to **60000**, sets the ceiling to **80000**, and sets the mode to **shape**.
- **list client-rate-class all**
  Displays a list of all client rate classs on the system.
- **delete client-rate-class sf1**
  Deletes the client rate class named **sf1** from the system.

Options

- **app-service**
  Specifies the name of the application service to which the object belongs. The default value is **none**. **Note:** If the **strict-updates** option is **enabled** on the application service that owns the object, you cannot modify or delete the object. Only the application service can modify or delete the object.
- **burst**
  Specifies in bytes the maximum amount of data that can reach the ceiling rate at one time. The default is **0** (zero).
- **ceiling**
  Specifies how far, beyond the value specified for the rate option, that traffic can flow when bursting. This number sets an absolute limit. No traffic can exceed this rate. The rate class might limit traffic throughput to the value of the rate option when there is high contention among siblings of a parent-child class hierarchy. The default value is the value of the rate option. The minimum value is **296** bp.
- **description**
  Specifies a description for the client rate class. The default is **none**.
- **dscp**
  Specifies six bits of DS field used as a codepoint to select the PHB (Per Hope Behavior) for a packet in each network node. The default is **-1**.
- **location-specific**
  Specifies whether or not this object contains one or more attributes with values that are specific to the location where the BIG-IP device resides. The location-specific attribute is either true or false. When using policy sync, mark an object as location-specific to prevent errors that can occur when policies reference objects, such as authentication servers, that are specific to a certain location.

- **[name]**
  Specifies a unique name to identify the client rate class.
- **mode**
  Specifies the mode to use for this client rate class. The options are:
  - **borrow**
    Allows traffic on the client rate class to borrow resources from other flows that are temporarily idle. Traffic that borrows resources is marked as nonconforming and receives a lower priority. This is the default.
  - **discard**
    Discards packets that do not conform to the specified traffic control descriptor.
  - **shape**
    Delays packets submitted for transmission until the packets conform to the specified flow paramaters
- **partition**
  Displays the partition within which this component resides. The default is **common**.
- **rate**
  Specifies the guaranteed throughput rate of the traffic handled by this rate class. You can configure the rate in bits per second (bps), kilobits per second (Kbps), megabits per second (Mbps), or gigabits per second (Gbps).
- **type**
  Specifies the service type in use for the client rate class. The options are:
  - **best-effort**
    Windows traffic control creates a flow for this client traffic class, and traffic on the flow is handled with the same priority as other Best Effort traffic. This is the default.
  - **controlled-load**
    Traffic control transmits a very high percentage of packets to the intended receivers. Packet loss for this type closely approximates the basic packet error rate of the transmission medium. Transmission delay for a very high percentage of the delivered packets does not greatly exceed the minimum transit delay experienced by any successfully delivered packet.
  - **guaranteed**
    Guarantees that datagrams arrive within a specified delivery time and will not be discarded due to queue overflows, provided that the flow of traffic stays within specified traffic parameters. This type is intended for applications that require guaranteed packet delivery.

See Also

tmsh

client-traffic-classifier

Configures client traffic classifier entries.

Syntax

Configure the **client-traffic-classifier** component within the **resource** module using the syntax shown in the following sections.

Create/Modify

```
create client-traffic-classifier [name]
modify client-traffic-classifier [name]
    app-service [[string] | none]
    entries [add | delete | modify | replace-all-with] {
      [name] {
      app-service [[string] | none]
      client-rate-class [[string] | none]
      dst-ip [[ipv4 address] | none]
      dst-mask [[integer] | none]
      dst-port [[integer] | none]
      protocol [[integer] | none]
      src-ip [[ipv4 address ] | none]
      src-mask [[integer] | none]
      src-port [[integer] | none]
      }
    location-specific [true | false]
}
edit client-traffic-classifier [ [ [name] | [glob] | [regex] ] ... ]
    all-properties
    non-default-properties
```

Display

```
list client-traffic-classifier
list client-traffic-classifier [ [ [name] | [glob] | [regex] ] ... ]
show running-config client-traffic-classifier
show running-config client-traffic-classifier [ [ [name] | [glob] | [regex] ] ... ]
    all-properties
    app-service
    non-default-properties
    one-line
    partition
show client-traffic-classifier
show client-traffic-classifier [name]
```

Delete

```
delete client-traffic-classifier [name]
```

Description

You can use the **client-traffic-classifier** component to configure a client traffic classifier, which is used by traffic control agent.

Examples

- **create client-traffic-classifier tf1{**
  entries entry1 {
  protocol "6"
  dst-ip "192.168.0.0"
  dst-mask "255.255.0.0"
  dst-port "0"
  client-rate-class "sf1"
  }
  entry2{protocol "6"
  src-ip "10.10.0.0"
  src-mask "255.255.255.0"
  client-rate-class "sf2"}}

  Creates a client traffic classifier named **tf1**, sets the entry to entry1, the protocol to **6**, the DST IP to **192.168.0.0**, the DST mask to **255.255.0.0**, the DST port to **0** (zero), and the client rate class to **sf1**.
- **list client-traffic-classifier all**
  Displays a list of all client traffic classifiers on the system.
- **modify client-traffic-classifier tf1 entries entry1 protocol 17**
  Modifies the client traffic classifier named **tf1**.
- **delete client-traffic-classifier tf1**
  Deletes the client traffic classifier named **tf1** from the system.

Options

- **app-service**
  Specifies the name of the application service to which the object belongs. The default value is **none**. **Note:** If the **strict-updates** option is **enabled** on the application service that owns the object, you cannot modify or delete the object. Only the application service can modify or delete the object.
- **dst-ip**
  Specifies the IP address of the receiver of the packet.
- **dst-mask**
  Specifies the subnet mask for the destination address.
- **dst-port**
  Specifies the 16-bit number to idenfity the sending port for either UDP or TCP network application.

- **location-specific**
  Specifies whether or not this object contains one or more attributes with values that are specific to the location where the BIG-IP device resides. The location-specific attribute is either true or false. When using policy sync, mark an object as location-specific to prevent errors that can occur when policies reference objects, such as authentication servers, that are specific to a certain location.
- **[name]**
  Specifies the name of the component.
- **partition**
  Displays the partition within which the component resides. The default is **Common**.
- **protocol**
  Specifies which traffic protocol to use in the filtering rule.
- **src-ip**
  Specifies the address from which the packet is being sent.
- **src-mask**
  Specifies the subnet mask for the source address.
- **src port**
  Specifies a 16-bit number to identify the sending port for either UDP or TCP network application.

See Also

tmsh

ipv6-leasepool

Configures a lease pool.

Syntax

Configure the **ipv6-leasepool** component within the **resource** module using the syntax shown in the following sections.

Create/Modify

```
create ipv6-leasepool [name]
modify ipv6-leasepool [name]
  options
    app-service [[string] | none]
    description [[string] | none]
    location-specific [true | false]
    members [add | delete | modify | replace-all-with] {
      [[first ip address in range] - [last ip address in range]]
    }
```

Display

```
list ipv6-leasepool
list ipv6-leasepool [ [ [name] | [glob] | [regex] ] ... ]
show running-config ipv6-leasepool
show running-config ipv6-leasepool [ [ [name] | [glob] | [regex] ] ... ]
    all-properties
    non-default-properties
    one-line
    partition
show ipv6-leasepool
show ipv6-leasepool [name]
```

Delete

```
delete ipv6-leasepool [name]
```

Description

Configures an IPv6 lease pool to create a collection of IPv6 addresses grouped as a single object. You can use a lease pool to associate that collection of IP addresses with a network access resource.

Examples

create ipv6-leasepool myipv6-leasepool {fd1f::1-fd1f::64}

Creates a ipv6-leasepool named **myipv6-leasepool** that contains the IPv6 addresses in the range **fd1f::1** - **fd1f::64**.

◆ Note

No spaces are allowed between the first IPv6 address, hyphen, and second IPv6 address.

Options

- **app-service**
  Specifies the name of the application service to which the object belongs. The default value is **none**. **Note:** If the **strict-updates** option is **enabled** on the application service that owns the object, you cannot modify or delete the object. Only the application service can modify or delete the object.
- **description**
  Specifies a unique description of the lease pool.
- **location-specific**
  Specifies whether or not this object contains one or more attributes with values that are specific to the location where the BIG-IP device resides. The location-specific attribute is either true or false. When using policy sync, mark an object as location-specific to prevent errors that can occur when policies reference objects, such as authentication servers, that are specific to a certain location.
- **[name]**
  Specifies a unique name for the lease pool.
- **members**
  Specifies a range of IPv6 addresses separated by a hyphen.
- **partition**
  Displays the partition within which the component resides. The default is **Common**.

See Also

apm profile, *virtual*

leasepool

Configures a lease pool.

Syntax

Configure the **leasepool** component within the **resource** module using the syntax shown in the following sections.

Create/Modify

```
create leasepool [name]
modify leasepool [name]
  options
    app-service [[string] | none]
    description [[string] | none]
    location-specific [true | false]
    members [add | delete | modify | replace-all-with] {
      [[first ip address in range] - [last ip address in range]]
    }
```

Display

```
list leasepool
list leasepool [ [ [name] | [glob] | [regex] ] ... ]
show running-config leasepool
show running-config leasepool [ [ [name] | [glob] | [regex] ] ... ]
    all-properties
    non-default-properties
    one-line
    partition
show leasepool
show leasepool [name]
```

Delete

```
delete leasepool [name]
```

Description

Configures a lease pool to create a collection of IPv4 addresses grouped as a single object. You can use a lease pool to associate that collection of IPv4 addresses with a network access resource.

Examples

create leasepool myleasepool {10.10.10.1-10.10.10.10}

Creates a leasepool named **myleasepool** that contains the IPv4 addresses in the range **10.10.10.1** - **10.10.10.10**.

◆ Note

No spaces are allowed between the first IPv4 address, hyphen, and second IPv4 address.

Options

- **app-service**
  Specifies the name of the application service to which the object belongs. The default value is **none**. **Note:** If the **strict-updates** option is **enabled** on the application service that owns the object, you cannot modify or delete the object. Only the application service can modify or delete the object.
- **description**
  Specifies a unique description of the lease pool.
- **location-specific**
  Specifies whether or not this object contains one or more attributes with values that are specific to the location where the BIG-IP device resides. The location-specific attribute is either true or false. When using policy sync, mark an object as location-specific to prevent errors that can occur when policies reference objects, such as authentication servers, that are specific to a certain location.
- **[name]**
  Specifies a unique name for the lease pool.
- **members**
  Specifies a range of IP addresses separated by a hyphen.
- **partition**
  Displays the partition within which the component resides. The default is **Common**.

See Also

apm profile, *virtual*

network-access

Configures general settings for a network access connection.

Syntax

Configure the **network-access** component within the **resource** module using the syntax shown in the following sections.

Create/Modify

```
create network-access [name]
modify network-access [name]
    app-service [[string] | none]
    address-space-dhcp-requests-excluded  [true | false]
    address-space-exclude-subnet [[string] | none]
    ipv6-address-space-exclude-subnet [[string] | none]
    address-space-include-dns-name [[string] | none]
    address-space-exclude-dns-name [[string] | none]
    address-space-include-subnet [[string] | none]
    ipv6-address-space-include-subnet [[string] | none]
    address-space-local-subnets-excluded  [true | false]
    address-space-loc-dns-servers-excluded  [true | false]
    address-space-protect [true | false]
    application-launch [[string] | none]
    application-launch-warning [true | false]
    auto-launch [true | false]
    client-interface-speed [[integer] | none]
    client-ip-filter-engine [true | false]
    client-power-management [ignore | prevent | terminate]
    client-proxy [true | false]
    client-proxy-address [ip addr]
    client-proxy-enforce-subnets [true | false]
    client-proxy-exclusion-list [[string] | none]
    client-proxy-local-bypass [true | false]
    client-proxy-port [[integer] | none]
    client-proxy-script [[string] | none]
    client-proxy-use-http-pac [true | false]
    client-proxy-use-local-proxy [true | false]
    client-traffic-classifier [[string] | none]
    compression [gzip | none]
    customization-group [[string] | none]
    description [[string] | none]
    dns-primary [ip addr]
    ipv6-dns-primary [ip addr]
    dns-secondary [ip addr]
    ipv6-dns-secondary [ip addr]
    dns-suffix [[string] | none]
    drive-mapping [[string] | none]
    dtls [true | false]
    dtls-port [[integer] | none]
    execute-logoff-scripts [true | false]
    idle-timeout-threshold [[integer] | none]
    idle-timeout-window [[integer] | none]
    leasepool-name [[string] | none]
    location-specific [true | false]
    ipv6-leasepool-name [[string] | none]
```

```
    microsoft-network-client [true | false]
    microsoft-network-server [true | false]
    network-tunnel [enabled | disabled]
    optimized-app [add | delete | modify | none | replace-all-with ]
    provide-client-cert [true | false]
    proxy-arp [true | false]
    split-tunneling [true | false]
    static-host [[string] | none]
    supported-ip-version [ipv4 | ipv4-ipv6]
    sync-with-active-directory [true | false]
    type [app-tunnel | last | network-access | remote-desktop | web-application]
    wins-primary [ip addr]
    wins-secondary [ip addr]
edit network-access [ [ [name] | [glob] | [regex] ] ... ]
    all-properties
    non-default-properties
```

Display

```
list network-access
list network-access [ [ [name] | [glob] | [regex] ] ... ]
show running-config network-access
show running-config network-access [ [ [name] | [glob] | [regex] ] ... ]
    all-properties
    non-default-properties
    one-line
    partition
show network-access
show network-access [name]
```

Delete

```
delete network-access [name]
```

Description

You can use the **network-access** component to configure the general settings for a network access connection.

Examples

- **create network-access mynetwork-access customization-group mynetaccess**
  Creates a network access connection configuration object named **mynetwork-access** that uses the policies in the customization group named **mynetaccess**.
- **delete network-access mynetwork-access**
  Deletes the network access connection configuration object named **mynetwork-access**.

Options

- **app-service**
  Specifies the name of the application service to which the object belongs. The default value is **none**. **Note:** If the **strict-updates** option is **enabled** on the application service that owns the object, you cannot modify or delete the object. Only the application service can modify or delete the object.
- **address-space-dhcp-requests-excluded**
  Specifies whether requests from IP addresses using DHCP are excluded from accessing the network. The default is **true**.
- **address-space-exclude-subnet**
  Specifies the IPv4 address spaces whose traffic you want to exclude from access to a subnet on the network. The default is **none**.
- **ipv6-address-space-exclude-subnet**
  Specifies the IPv6 address spaces whose traffic you want to exclude from access to a subnet on the network. The default is **none**.
- **address-space-include-dns-name**
  Specifies a list of domain names describing the target LAN DNS addresses for split tunneling only. You can add multiple address spaces to the list. For each address space, type the domain name, in the form **site.siterequest.com** or ***.siterequest.com**. The default is **none**.
- **address-space-exclude-dns-name**
  Specifies the DNS address spaces whose traffic you want to exclude from access to a subnet on the network. You can add multiple address spaces to the list. For each address space, type the domain name, in the form **site.siterequest.com** or ***.siterequest.com**. The default is **none**.
- **address-space-include-subnet**
  Specifies a list of IPv4 addresses or address/mask pairs describing the target LAN. When using split tunneling, only the traffic to these addresses and network segments goes through the tunnel configured for Network Access. You can add multiple address spaces to the list. For each address space, type the IPv4 address and network mask. The default is **none**.
- **ipv6-address-space-include-subnet**
  Specifies a list of IPv6 addresses or address/mask pairs describing the target LAN. When using split tunneling, only the traffic to these addresses and network segments goes through the tunnel configured for Network Access. You can add multiple address spaces to the list. For each address space, type the IPv6 address and network mask. The default is **none**.
- **address-space-local-subnets-excluded**
  Specifies whether to exclude local access to any host or subnet in routes that you have specified in the client routing table. The default is **false**. When you set this option to **true**, the system does not support integrated IP filtering.

- **address-space-loc-dns-servers-excluded**
  Specifies whether to exclude local access to DNS servers configured on client prior to establishing network access connection. The default is **false**.
- **address-space-protect**
  Specifies whether the IP address spaces whose traffic is forced through the tunnel are protected. The default is **false**.
- **app-service**
  The default is **none**.
- **application-launch**
  Specifies the applications to launch when the client accesses the network. The default is **none**.
- **application-launch-warning**
  Specifies whether the user is warned that an application is being launched. The default is **true**.
- **auto-launch**
  Specifies whether NA resource is to be launched automatically from full webtop. The default is **false**.
- **client-interface-speed**
  Specifies the baud rate of the client interface with the network. The default is **100000000**.
- **client-ip-filter-engine**
  Specifies whether the client IP address is filtered. The default is <false>.
- **client-power-management**
  Specifies how to interact with Windows power management features.
  - **prevent**
    Prevents Windows from entering standby/hibernate during connection.
  - **terminate**
    Terminate network access connection if Windows is entering standby/hibernate
  - **ignore**
    Do nothing. Ignore power management events. This is the default value.
- **client-proxy**
  Specifies whether this resource handles a client proxy. The default is **false**.
- **client-proxy-address**
  Specifies the IP address of the proxy client. The default is **any6**.
- **client-proxy-enforce-subnets**
  Specifies whether address space subnets must be enforced in proxy auto-configuration. The default is **true**.

- **client-proxy-exclusion-list**
  Specifies the Web addresses that do not need to be accessed through your proxy server. You can use wild cards to match domain and host names or addresses, for example, **www.*.com**, **128.***, **240.8**, **8.**, **mygroup.***, and ***.***. The default is **none**.
- **client-proxy-local-bypass**
  Specifies whether you want to allow local (intranet) addresses to bypass the proxy server. The default is **false**.
- **client-proxy-port**
  Specifies the port number of the proxy server you want Network Access clients to use to connect to the Internet. The default is **0** (zero).
- **client-proxy-script**
  Specifies the URL for a proxy auto-configuration script, if one is used with this connection. The default is **none**.
- **client-proxy-use-http-pac**
  Specifies whether the browser uses **http://** to locate the proxy the autoconfig file, instead of **file://**. Set this to **true** for applications, like Citrix MetaFrame, that cannot use the client proxy autoconfig script when the browser attempts to use the prefix file:// to locate the script. The default is **false**.
- **client-proxy-use-local-proxy**
  Specifies whether the browser uses the proxy configured on client prior to establishing network access connection. The default is **false**.
- **client-traffic-classifier**
  Specifies a client traffic classifier to use with this network access connection. The default is **none**.
- **compression**
  Specifies whether you want to compress all traffic between the Network Access client and the controller. The default is **none**.
- **customization-group**
  Specifies the customization group that defines the policies that apply to network access. This option is required.
- **description**
  Specifies a unique description of the network access configuration object. The default is **none**.
- **dns-primary**
  For split tunneling, specifies the IPv4 address of the primary name server that is conveyed to the remote access point for IPv4 traffic. The default is **any6**.
- **ipv6-dns-primary**
  For split tunneling, specifies the IPv6 address of the primary name server that is conveyed to the remote access point for IPv6 traffic. The default is **any6**.
- **dns-secondary**
  For split tunneling, specifies the IPv4 address of the secondary name server that is conveyed to the remote access point for IPv4 traffic. The default is **any6**.

- **ipv6-dns-secondary**
  For split tunneling, specifies the IPv6 address of the secondary name server that is conveyed to the remote access point for IPv6 traffic. The default is **any6**.
- **dns-suffix**
  Type in a DNS suffix to send to the client. If this field is left blank, the controller sends its own DNS suffix. You can specify multiple default domain suffixes separated with commas. The default is **none**.
- **drive-mapping**
  For split tunneling, specifies the drive to which this resource provides a network access connection. The default is **none**.
- **dtls**
  Specifies whether the network access connection uses Datagram Transport Level Security (DTLS). DTLS uses UDP instead of TCP, to provides better throughput for high demand applications like VoIP or streaming video, especially with lossy connections. The default is **false**.
- **dtls-port**
  Specifies the port number that the network access resource uses for secure UDP traffic with DTLS. The default is **4433**.
- **execute-logoff-scripts**
  Specifies whether the system to executes logoff scripts (configured on the Active Directory domain) when the connection is terminated. The default is **false**.
- **idle-timeout-threshold**
  Defines the average byte rate that either ingress or egress tunnel traffic must exceed for the tunnel to update a session. If the average byte rate falls below the specified threshold, the system applies the inactivity timeout, which is defined in the session's Access Profile. The default is **0** (zero).
- **idle-timeout-window**
  Defines the value that the system uses to calculate the Exponential Moving Average (EMA) byte rate of ingress and egress tunnel traffic. The default is **0** (zero).
- **leasepool-name**
  Specifies the IPv4 lease pools that the user can access with this network access connection. The default is **none**.
- **ipv6-leasepool-name**
  Specifies the IPv6 lease pools that the user can access with this network access connection. The default is **none**.
- **location-specific**
  Specifies whether or not this object contains one or more attributes with values that are specific to the location where the BIG-IP device resides. The location-specific attribute is either true or false. When using policy sync, mark an object as location-specific to prevent errors that can occur when policies reference objects, such as authentication servers, that are specific to a certain location.

- **microsoft-network-client**
  Specifies whether the client PC can access remote resources over a VPN connection. The default is **true**.
- **microsoft-network-server**
  Specifies whether the server can access remote resources over a VPN connection. The default is **false**.
- **network-tunnel**
  Enables or disables the network tunnel. The default is **enabled**.
- **optimized-app**
  Specifies the optimized applications that you want to users to access using this network access connection resource. You can add, delete, modify, or replace the current optimized applications. The default is **none**.
- **partition**
  Displays the partition within which this network access connection component resides. The default is **Common**.
- **provide-client-cert**
  Specifies whether client certificates are required to establish an SSL connection. You can set this option to **false** if the client certificates are only requested in an SSL connection. In this case, the client is configured to not send client certificates. The default is **true**.
- **proxy-arp**
  Select **Enable** to enable Proxy ARP for this network access resource. When you implement Proxy ARP for a network access resource, remote VPN tunnel clients can use IP addresses from the LAN IP subnet without additional network infrastructure changes. Ranges of IP addresses from the LAN subnet can be configured in the lease pools and assigned to tunnel clients. When a host on the LAN sends traffic to a tunnel client, an ARP query is sent to request the client address. Access Policy Manager then responds with its own MAC address. Traffic is then sent to network access and forwarded to the client over the network access tunnel. No configuration changes are required on devices other than the Access Policy Manager.
  See your Network Access documentation for more information about Proxy ARP configuration. The default is **false**.
- **split-tunneling**
  Specifies whether only traffic targeted to a specified address space is sent over the network access tunnel. With split tunneling, all other traffic bypasses the tunnel. The default is **false**. When you set this option to **true**, all traffic passing over the network access connection uses this setting.
- **static-host**
  Specifies the static hosts to which this resource provides a network access connection. The default is **none**.
- **supported-ip-version**
  Specifies the supported IP protocol version. The default is **ipv4**.

- **sync-with-active-directory**
  Specifies whether you want the network access connection to emulate the Windows logon process for a client on an Active Directory domain. The default is **false**.
  When this option is set to **true**, network policies are synchronized when the connection is established, or at logoff. The following items are synchronized:
  - Logon scripts are started as specified in the user profile.
  - Drives are mapped as specified in the user profile.
  - Group policies are synchronized as specified in the user profile. Group Policy logon scripts are started when the connection is established, and Group Policy logoff scripts are run when the network access connection is stopped.
- **type**
  Specifies the type of network access connection this component provides. The default is **network-access**.
- **wins-primary**
  Specifies the primary IP address to which this resource provides a network access connection. The default is **any6**.
- **wins-secondary**
  Specifies the secondary IP address to which this resource provides a network access connection. The default is **any6**.

See Also

tmsh

portal-access

Configures a portal access resource.

Syntax

Configure the **portal-access** component within the **resource** module using the syntax shown in the following sections.

Create/Modify

```
create portal-access [name]
modify portal-access [name]
    acl-order [integer]
    application-uri [string] | none]
    app-service [[string] | none]
    css-patching [true | false]
    customization-group [string] | none]
    description [string] | none]
    flash-patching [true | false]
    host-replace-string [string] | none]
    host-search-strings [string] | none]
    html-patching [true | false]
    items [add | delete | modify | replace-all-with] {
      [string]
    }
    javascript-patching [true | false]
    location-specific [true | false]
    patching-type [full-patch | min-patch]
    path-match-case [true | false]
    proxy-host [string] | none]
    proxy-port [string] | none]
    publish-on-webtop [true | false]
    scheme-patching [true | false]
edit portal-access [ all-properties | non-default-properties ]
    all-properties
    non-default-properties
```

Display

```
list portal-access
list portal-access [ [ [name] | [glob] | [regex] ] ... ]
show running-config portal-access
show running-config portal-access [ [ [name] | [glob] | [regex] ] ... ]
    all-properties
    non-default-properties
    one-line
    partition
show portal-access
show portal-access [name]
```

Delete

```
delete portal-access [name]
```

Description

You can use the **portal-access** component to specify a portal access resource.

Examples

item **create portal-access myportalaccess acl-order 14 patching-type full-patch items add { item1 { host www.mywebsite.com paths /* }}**

Creates a portal access resource named **myportalaccess**.

item **delete portal-access myportalaccess**

Deletes the portal access resource named **myportalaccess**.

Options

- **acl-order**
  Specifies the order of this portal access in Access Policy Manager ACL lists. This option is required.
- **application-uri**
- **app-service**
  Specifies the name of the application service to which the object belongs. The default value is **none**. **Note:** If the **strict-updates** option is **enabled** on the application service that owns the object, you cannot modify or delete the object. Only the application service can modify or delete the object.
- **css-patching**
  Specifies whether the response content type CSS is patched. The default is **true**.
- **customization-group**
  The customization group is created automatically if not specified.
- **description**
  Specifies a description of the resource. The default is **none**.
- **flash-patching**
  Specifies whether the system patches Flash content. The default is **true**.
- **host-replace-string**
  Specifies the replacement host string, when you specify **minimal** for the **patching-type** option.
- **host-search-strings**
  Specifies the host string to replace, when you specify **minimal** for the **patching-type** option.
- **html-patching**
  Specifies whether the system patches HTML content. The default is **true**.

- **items**
  Configures the host name or IP address, the network mask (if the resource is a network), the port, and any paths specified for a portal access resource. The default is **none**.
- **javascript-patching**
  Specifies whether the system patches JavaScript content. The default is **true**.
- **location-specific**
  Specifies whether or not this object contains one or more attributes with values that are specific to the location where the BIG-IP device resides. The location-specific attribute is either true or false. When using policy sync, mark an object as location-specific to prevent errors that can occur when policies reference objects, such as authentication servers, that are specific to a certain location.
- **[name]**
  Specifies a unique name for the component.
- **patching-type**
  Specifies whether this resource provides minimal or full path patching.
- **path-match-case**
  Specifies whether the application URI is case-sensitive. The default is **true**.
- **proxy-host**
  Specifies the proxy host that the portal access uses. The default is **none**. If you configure this option, you must also configure the option **proxy-port**.
- **proxy-port**
  Specifies the port that the portal access proxy uses. The default is **none**. Configure this option, only when you configure the option **proxy-host**.
- **publish-on-webtop**
  Specifies whether to publish this resource on the webtop. The default is **false**. If you set this option to **true**, you must also specify the Application URI using the **application-uri** option.
- **scheme-patching**
  Specifies whether this resource replaces all HTTP scheme addresses with HTTPS scheme addresses. This option is effective only when minimal patching is selected for patching-type. The default is **false**.

See Also

tmsh

sandbox

Configures a sandbox.

Syntax

Configure the **sandbox** component within the **resource** module using the syntax shown in the following sections.

Create

The CREATE command is currently not available. However, a number of sandboxes have already been created. Use these to upload files.

Modify

```
modify sandbox [name]
  options
    base-uri [string]
    description [[string] | none]
    files [add | delete | modify | replace-all-with] {
      [item name] {
        content-type [string]
        filename [string]
        file-type [citrix-bundle | customization | unknown]
        folder [string]
        local-path [string]
        name [string]
      }
    }
```

Display

```
list sandbox
list sandbox [ [ [name] | [glob] | [regex] ] ... ]
    all-properties
    non-default-properties
    one-line
    partition
```

Description

Configures a sandbox and its files. A sandbox is a container for files stored on the BIG-IP, to which you want to provide client access.

Examples

modify sandbox hosted-content files add { BIGIPEdgeClient.exe { folder /client local-path /tmp/BIGIPEdgeClient.exe } }

Adds a file called BIGIPEdgeClient.exe to sandbox named **hosted-content**. The virtual path to this file consists of the sandbox's base-uri, the file's folder, and the name of the file. Putting these components together, the virtual path for the uploaded file is /public/share/client/BIGIPEdgeClient.exe, where /public/share is the base-uri, /client is the folder, and BIGIPEdgeClient.exe is the filename. The local-path indicates the location of the file on the disk drive to be added into the sandbox.

◆ Note

The file you add must already be on the BIG-IP system.

Options

- **base-uri**
  Specifies the first component of the virtual path to the sandbox file. The base-uri for sandbox "hosted-content" is /public/share. The virtual path to a sandbox box file is made up of three components:
  base-uri/folder/filename
  All files in a sandbox share the same base-uri, but the folder can be different for each file.
- **description**
  Specifies a unique description about the sandbox.
- **files**
  Specifies the list of files in the sandbox.
- **item name**
  Specifies the name of an item in the list of files. You can use the original filename as the item name. Each item name in a sandbox must be unique.
- **content-type**
  Specifies the content-type field in a HTTP header such as "image/gif" or "text/plain". If none is provided, tmsh will try its best to provide this value.
- **filename**
  Specifies the last component of the virtual path to the sandbox file. We recommend that you use the filename of the original file for this name.
- **file-type**
  Specifies the F5 file type. Currently there are only three types: unknown, citrix-bundle, and customization. No value is required if a file is uploaded to sandbox for "citrix-client-bundle", since this sandbox is the repositories for F5 specific type of file. However, for files uploaded to sandbox "hosted-content" if no value is provided, the file type defaults to "unknown".
- **folder**
  Specifies the second component of the virtual path to the sandbox file.
- **local-path**
  Specifies the location of the file to be inserted into the sandbox. This file must be on the BIG-IP already.

- **name**
  Specifies a value for the underlying file object. Use this only if you are trying to add more than one sandbox file in a modify command. Otherwise, don't specify a value for this attribute. The value must be specified as follows: full path of sandbox name:item name. For example, if the sandbox name is '/Common/hosted-content' and the item name is 'index.html', the value should be '/Common/hosted-content:index.html'.

See Also

webtop, *webtop-link*

webtop

Configures a webtop resource.

Syntax

Configure the **webtop** component within the **resource** module using the syntax shown in the following sections.

Create/Modify

```
create webtop [name]
modify webtop [name]
    app-service [[string] | none]
    customization-group [string]
    description [[string] | none]
    location-specific [true | false]
    minimize-to-tray [false | true]
    portal-access-start-uri [[string] | none]
    webtop-type [full | last | network-access | portal-access]
    warn-when-closed [false | true]
edit webtop [ [ [name] | [glob] | [regex] ] ... ]
    all-properties
    non-default-properties
```

Display

```
list webtop
list webtop [ [ [name] | [glob] | [regex] ] ... ]
show running-config webtop
show running-config webtop [ [ [name] | [glob] | [regex] ] ... ]
    all-properties
    non-default-properties
    one-line
show webtop
show webtop [name]
```

Delete

```
delete webtop [name]
```

Description

Configures the settings necessary to define the webtop assigned to the end-user as part of the access policy execution.

Examples

- **create webtop mynawebtop { customization-group mywebtopcg1 minimize-to-tray false }**
  Creates a webtop named **mynawebtop** with the customization group **mywebtopcg1** and the network access **minimize-to-tray** option set to false.
- **create webtop mywawebtop { customization-group mywebtopcg1 portal-access-start-uri ‘"http://www.siterequest.com"’ }**
  Creates a webtop named **mywawebtop** with the customization group **mywebtopcg1** and the starting URI for the portal access of **http://www.siterequest.com**.

Options

- **app-service**
  Specifies the name of the application service to which the object belongs. The default value is **none**. **Note:** If the **strict-updates** option is **enabled** on the application service that owns the object, you cannot modify or delete the object. Only the application service can modify or delete the object.
- **customization-group**
  Specifies the customization settings for the webtop.

◆ Note

*You must create a customization group of type **webtop** before you can create a webtop resource. This option is required.*

- **description**
  Specifies a description of the resource. The default is **none**.
- **portal-access-start-uri**
  Specifies the URI that the webtop starts. You can only configure this option if you have configured the **webtop-type** option for **portal-access**.
- **location-specific**
  Specifies whether or not this object contains one or more attributes with values that are specific to the location where the BIG-IP device resides. The location-specific attribute is either true or false. When using policy sync, mark an object as location-specific to prevent errors that can occur when policies reference objects, such as authentication servers, that are specific to a certain location.
- **minimize-to-tray**
  Specifies whether the network access window (launched from the full webtop) is minimized to the system tray automatically after the network access connection starts. The default is **true**.
  You can configure this option only if you configured the **webtop-type** option as **network-access** or **full**. With a network access webtop, the

webtop automatically minimizes to the tray. With a full webtop, the webtop minimizes to the system tray only after the network access connection is started.

- **warn-when-closed**
  Specifies whether the network access window (launched from the full webtop) should display a warning message when the webtop closes. You can configure this option only if you configured the **webtop-type** option as **full**.
- **webtop-type**
  Specifies the type of webtop this resource creates. The options are:
  - **full**
    A webtop to which you assign a single network access resource, multiple portal access resources, and multiple application access app tunnel resources, or any combination of the three types. This is the default.
  - **last**
  - **network-access**
    A webtop to which you assign only a single network access resource.
  - **portal-access**
    A webtop to which you assign only portal access resources.

See Also

tmsh

webtop-link

Configures a webtop link resource.

Syntax

Configure the **webtop-link** component within the **resource** module using the syntax shown in the following sections.

Create/Modify

```
create webtop-link [name]
modify webtop-link [name]
    application-uri [string]
    app-service [[string] | none]
    customization-group [string]
    description [[string] | none]
    location-specific [true | false]
edit webtop-link [ [ [name] | [glob] | [regex] ] ... ]
    all
```

Display

```
list webtop-link
list webtop-link [ [ [name] | [glob] | [regex] ] ... ]
show running-config webtop-link
show running-config webtop-link [ [ [name] | [glob] | [regex] ] ... ]
    all-properties
    non-default-properties
    one-line
show webtop-link
show webtop-link [name]
```

Delete

```
delete webtop-link [name]
```

Description

Configures the settings necessary to define a link to a webtop that is displayed to the end-user as part of the access policy execution.

Examples

- **create webtop-link mywebtoplinkcg1 application-uri "http://www.externalsite.com/"**
  Creates a webtop named **mywebtoplinkcg1** with the application-uri of **http://www.externalsite.com/**.

Options

- **application-uri**
  Specifies the application URI of the external portal to which this resource provides access for this webtop link. This is a required setting.
- **app-service**
  Specifies the name of the application service to which the object belongs. The default value is **none**. **Note:** If the **strict-updates** option is **enabled** on the application service that owns the object, you cannot modify or delete the object. Only the application service can modify or delete the object.
- **customization-group**
  Specifies the customization settings for the webtop.

◆ Note

*You must create a customization group of type **webtop** before you can create a webtop resource. If you do not specify a customization group, a group will be created automatically.*

- **description**
  Specifies a description of the resource. The default is **none**.
- **location-specific**
  Specifies whether or not this object contains one or more attributes with values that are specific to the location where the BIG-IP device resides. The location-specific attribute is either true or false. When using policy sync, mark an object as location-specific to prevent errors that can occur when policies reference objects, such as authentication servers, that are specific to a certain location.

See Also

tmsh

38

apm resource remote-desktop

- Introducing the apm resource remote-desktop module
- Alphabetical list of components

Introducing the apm resource remote-desktop module

You can use the tmsh components that reside within the apm resource remote-desktop module to configure BIG-IP® Access Policy Manager®. For more information about the tmsh hierarchical structure, see Chapter 2, *Understanding and Using the Traffic Management Shell*.

Alphabetical list of components

The remainder of this chapter lists the tmsh components that are available in the apm resource remote-desktop module.

citrix

Configures a Citrix remote desktop resource configuration object.

Syntax

Configure the **citrix** component within the **resource remote desktop** module using the syntax shown in the following sections.

Create/Modify

```
create citrix [name]
modify citrix [name]
    app-service [[string] | none]
    auto-logon [enabled | disabled]
    customization-group [add | delete | modify | replace-all-with] {
      [name] {
          caption [[string] | none]
          detailed-description [[string] | none]
       }
    }
    description [[string] | none]
    domain-source [session.logon.last.domain | none]
    enable-serverside-ssl [enabled | disabled]
    pool [pool name]
    host [fqdn]
    ip [ip address]
    location-specific [true | false]
    password-source [session.logon.last.password | none]
    port [[string] | none]
    username-source [session.logon.last.username | none]
edit citrix [ [ [name] | [glob] | [regex] ] ... ]
    all-properties
    non-default-properties
```

Display

```
list citrix
list citrix [ [ [name] | [glob] | [regex] ] ... ]
show running-config citrix
show running-config citrix [ [ [name] | [glob] | [regex] ] ... ]
    all-properties
    non-default-properties
show citrix
show citrix [name]
```

Delete

```
delete citrix [name]
```

Description

```
You can use the B<citrix> component to configure a Citrix remote desktop resource.
```

Examples

- **create citrix mycitrix { ip 172.29.67.130 }**
  Creates a Citrix remote desktop resource named **mycitrix** with Citrix XML Broker server specified as IP address **172.29.67.130**.
- **create citrix mycitrix { host mycitrix.mycompany.com auto-logon enabled }**
  Creates a Citrix resource with Citrix XML Broker server specified as hostname **mycitrix.mycompany.com** and auto-logon enabled with APM credentials (that user types on Logon Page).
- **create citrix mycitrix { pool /Common/mycitrix-pool enable-serverside-ssl enabled }**
  Creates a Citrix resource with Citrix XML Broker server(s) specified in pool named **/Common/mycitrix-pool** and SSL communication enabled to the server(s) (SSL should also be enabled on the servers and APM virtual should have serverssl profile).

Options

- **app-service**
  Specifies the name of the application service to which the object belongs. The default value is **none**. **Note:** If the **strict-updates** option is **enabled** on the application service that owns the object, you cannot modify or delete the object. Only the application service can modify or delete the object.
- **auto-logon**
  Enables or disables automatic log on to the Citrix server. If you enable this option, you must also provide values for the **username-source**, **password-source**, and **domain-source** options. The default is **disabled**.
- **customization-group**
  Specifies whether customization groups are applied to the Citrix remote desktop. You can add, modify, or delete customization groups. You can also replace all current customization groups with new customization groups. The default is **none**.
- **description**
  Specifies a description for your Citrix remote desktop. The default is **none**.
- **domain-source**
  Specifies the Session variable used as a source for the **auto-logon** user password. The default is **session.logon.last.domain**.
- **enable-serverside-ssl**
  Enables or disables SSL capabilities between the BIG-IP system and the Citrix server. When enabled, the port number automatically changes to **443**. The default is **disabled**.
- **pool**
  Specifies the pool name that contains your Citrix XML Broker server(s). You must use one of these options to specify the server address: **pool**, **host**, or **ip**.

- **host**
  Specifies the hostname of your Citrix XML Broker server. You must use one of these options to specify the server address: **pool**, **host**, or **ip**.
- **ip**
  Specifies the IP address of your Citrix XML Broker server. You must use one of these options to specify the server address: **pool**, **host**, or **ip**.
- **location-specific**
  Specifies whether or not this object contains one or more attributes with values that are specific to the location where the BIG-IP device resides. The location-specific attribute is either true or false. When using policy sync, mark an object as location-specific to prevent errors that can occur when policies reference objects, such as authentication servers, that are specific to a certain location.
- **[name]**
  Specifies an object name. This option is required; however, the parameter **name** is implicit and must not be typed in the syntax.
- **password-source**
  Specifies the session variable that is used as a source for the **auto-logon** password. The default is **session.logon.last.password**.
- **port**
  Specifies the port for your Citrix server. The default is **80**.
- **username-source**
  Specifies the session variable that is used as a source for the **auto-logon** user name. The default is **session.logon.last.username**.

See Also

citrix-client-bundle, *citrix-client-package-file*, *rdp*, *vmware-view*, *quest*

citrix-client-bundle

Configures a Citrix Client Bundle remote desktop resource configuration object.

Syntax

Configure the **citrix-client-bundle** component within the **resource remote desktop** module using the syntax shown in the following sections.

Create/Modify

```
create citrix-client-bundle [name]
modify citrix-client-bundle [name]
    app-service [[string] | none]
    download-url [[url] | none]
    packages [[string] | none]
    windows-download-url [[url] | none]
    windows-min-version [[string] | none]
    windows-package [[string] | none]
edit citrix-client-bundle [ [ [name] | [glob] | [regex] ] ... ]
    all-properties
    non-default-properties
```

Display

```
list citrix-client-bundle
list citrix-client-bundle [ [ [name] | [glob] | [regex] ] ... ]
show running-config citrix-client-bundle
show running-config citrix-client-bundle [ [ [name] | [glob] | [regex] ] ... ]
    all-properties
    non-default-properties
    one-line
    partition
show citrix-client-bundle
show citrix-client-bundle [name]
```

Delete

```
delete citrix-client-bundle [name]
```

Description

You can use the **citrix-client-bundle** component to configure a Citrix Client Bundle remote desktop resource.

Examples

```
create citrix-client_bundle myccb { windows-min-version xp }
```

Creates a Citrix Client Bundle remote desktop resource named **myccb** that can be downloaded from **receiver.citrix.com** (the default value), where the client must have at least Windows XP installed.

Options

- **app-service**
  Specifies the name of the application service to which the object belongs. The default value is **none**. **Note:** If the **strict-updates** option is **enabled** on the application service that owns the object, you cannot modify or delete the object. Only the application service can modify or delete the object.
- **download-url**
  Specifies the default location **receiver.citrix.com** from which to download the Citrix installation package.
- **packages**
  Specifies the location from which to download client installer package. The default is **none**.
- **[name]**
  Specifies an object name. This option is required; however, the parameter **name** is implicit and must not be typed in the syntax.
- **windows-download-url**
  Specifies the location from which to download the Windows version. You can provide a value for either the **windows-download-url** or **windows-package** option, but not both. The default is **none**.
- **windows-min-version**
  Specifies the oldest version of the Citrix client that can be used with this remote desktop resource. The default is **none**.
- **windows-package**
  Specifies the location from which to download the Windows package. You can provide a value for either the **windows-package** or **windows-download-url** option, but not for both. The default is **none**.

See Also

citrix, *citrix-client-package-file*, *rdp*

citrix-client-package-file

Configures a Citrix client package file configuration object.

Syntax

Configure the **citrix-client-package-file** component within the **resource remote desktop** module using the syntax shown in the following sections.

Create/Modify

```
create citrix-client-package-file [name]
modify citrix-client-package-file [name]
    app-service [[string] | none]
    location-specific [true | false]
    original-file-name [[string] | none]
    source-path [[string] | none]
edit citrix-client-package-file [ [ [name] | [glob] | [regex] ] ... ]
    all-properties
    non-default-properties
```

Display

```
list citrix-client-package-file
list citrix-client-package-file [ [ [name] | [glob] | [regex] ] ... ]
show running-config citrix-client-package-file
show running-config citrix-client-package-file [ [ [name] | [glob] | [regex] ] ... ]
    all-properties
    non-default-properties
    one-line
    partition
```

Delete

```
delete citrix-client-package-file [name]
```

Description

You can use the **citrix-client-package-file** component to configure access to a Citrix client package file.

Examples

- **create citrix-client-package myccpackage { source-path www.siterequest.citrix_download.com }**
  Creates a Citrix client package remote desktop resource named **myccpackage** that is available from **www.siterequest.citrix_download.com**.

Options

- **[name]**
  Specifies an object name. This option is required; however, the parameter **name** is implicit and must not be typed in the syntax.
- **app-service**
  Specifies the name of the application service to which the object belongs. The default value is **none**. **Note:** If the **strict-updates** option is **enabled** on the application service that owns the object, you cannot modify or delete the object. Only the application service can modify or delete the object.
- **location-specific**
  Specifies whether or not this object contains one or more attributes with values that are specific to the location where the BIG-IP device resides. The location-specific attribute is either true or false. When using policy sync, mark an object as location-specific to prevent errors that can occur when policies reference objects, such as authentication servers, that are specific to a certain location.
- **original-file-name**
  Specifies the original file name of the Citrix Installation package file name to download. The default is **none**.
- **source-path**
  Specifies the location from which to download the Citrix client package file. This option is required.

See Also

citrix, *citrix-client-bundle*, *rdp*

quest

Configures a Quest vWorkspace remote desktop resource configuration object.

Syntax

Configure the **quest** component within the **resource remote desktop** module using the syntax shown in the following sections.

Create/Modify

```
create quest [name]
modify quest [name]
    app-service [[string] | none]
    auto-logon [enabled | disabled]
    customization-group [add | delete | modify | replace-all-with] {
      [name] {
          caption [[string] | none]
          detailed-description [[string] | none]
       }
    }
    description [[string] | none]
    domain-source [session.logon.last.domain | none]
    enable-serverside-ssl [enabled | disabled]
    pool [pool name]
    host [fqdn]
    ip [ip address]
    location-specific [true | false]
    password-source [session.logon.last.password | none]
    port [[string] | none]
    username-source [session.logon.last.username | none]
edit quest [ [ [name] | [glob] | [regex] ] ... ]
    all-properties
    non-default-properties
```

Display

```
list quest
list quest [ [ [name] | [glob] | [regex] ] ... ]
show running-config quest
show running-config quest [ [ [name] | [glob] | [regex] ] ... ]
    all-properties
    non-default-properties
show quest
show quest [name]
```

Delete

```
delete quest [name]
```

Description

You can use the B<quest> component to configure a Quest vWorkspace remote desktop resource.

Examples

- **create quest myquest { ip 172.29.67.130 }**
  Creates a Quest vWorkspace remote desktop resource named **myquest** with the Quest vWorkspace connection broker server specified as IP address **172.29.67.130**.
- **create quest myquest { host myquest.mycompany.com auto-logon enabled }**
  Creates a Quest vWorkspace resource with the Quest vWorkspace connection broker server specified as hostname **myquest.mycompany.com** and with auto-logon enabled using the credentials that the user types into the access policy Logon Page.
- **create quest myquest { pool /Common/myquest-pool enable-serverside-ssl enabled }**
  Creates a Quest vWorkspace resource with the Quest vWorkspace connection broker servers specified in a pool named **/Common/myquest-pool** and with SSL communication enabled to the servers. **Note:** SSL should also be enabled on the servers themselves and the APM virtual server should specify a server SSL profile.

Options

- **app-service**
  Specifies the name of the application service to which the object belongs. The default value is **none**. **Note:** If the **strict-updates** option is **enabled** on the application service that owns the object, you cannot modify or delete the object. Only the application service can modify or delete the object.
- **auto-logon**
  Enables or disables automatic log on to the Quest vWorkspace connection broker server. If you enable this option, you must also provide values for the **username-source**, **password-source**, and **domain-source** options. The default is **disabled**.
- **customization-group**
  Specifies whether customization groups are applied to the Quest vWorkspace resource. You can add, modify, or delete customization groups. You can also replace all current customization groups with new customization groups. The default is **none**.
- **description**
  Specifies a description for your Quest vWorkspace remote desktop. The default is **none**.

- **domain-source**
  Specifies the session variable to use as a source for the **auto-logon** user password. The default is **session.logon.last.domain**.
- **enable-serverside-ssl**
  Enables or disables SSL capabilities between the BIG-IP system and the Quest vWorkspace connection broker server. When enabled, the port number automatically changes to **443**. The default is **disabled**.
- **pool**
  Specifies the pool name that contains your Quest vWorkspace connection broker servers. (You must specify the server address using one of these options: **pool**, **host**, or **ip**.)
- **host**
  Specifies the hostname of your Quest vWorkspace connection broker server. (You must specify the server address using one of these options: **pool**, **host**, or **ip**.)
- **ip**
  Specifies the IP address of your Quest vWorkspace connection broker server. (You must specify the server address using one of these options: **pool**, **host**, or **ip**.)
- **location-specific**
  Specifies whether or not this object contains one or more attributes with values that are specific to the location where the BIG-IP device resides. The location-specific attribute is either true or false. When using policy sync, mark an object as location-specific to prevent errors that can occur when policies reference objects, such as authentication servers, that are specific to a certain location.
- **[name]**
  Specifies an object name. This option is required. **Note:** The parameter **name** is implicit. Do not type **name** in the syntax.
- **password-source**
  Specifies the session variable to use as a source for the **auto-logon** password. The default is **session.logon.last.password**.
- **port**
  Specifies the port for your Quest vWorkspace connection broker server. The default is **8080**.
- **username-source**
  Specifies the session variable to use as a source for the **auto-logon** user name. The default is **session.logon.last.username**.

See Also

citrix, *rdp*, *vmware-view*

rdp

Configures a Microsoft Remote Desktop Protocol (MSRDP) configuration object.

Syntax

Configure the **rdp** component within the **resource remote desktop** module using the syntax shown in the following sections.

Create/Modify

```
create rdp [name]
modify rdp [name]
    acl-order [[integer] | none]
    application [[string] | none]
    app-service [[string] | none]
    auto-logon [enabled | disabled]
    color-depth [4 | 8 | 16 | 24]
    customization-group [add | delete | modify | replace-all-with] {
      [name] {
          app-service [[string] | none]
          caption [[string] | none]
          detailed-description [[string] | none]
       }
    }
    description [[string] | none]
    domain-source [session.logon.last.domain | none]
    host [fqdn]
    ip [ip address]
    java-client [enabled | disabled]
    location-specific [true | false]
    log [config | none | packet | summary | verbose]
    password-source [session.logon.last.password | none]
    port [[integer] | none]
    rdp-cache-bitmaps [true | false]
    rdp-show-contents-while-dragging [true | false]
    rdp-show-desktop-wallpaper [true | false]
    rdp-show-themes [true | false]
    rdp-window-animations [true | false]
    redirect-com-parts [true | false]
    redirect-drives [true | false]
    redirect-keyboard-commands [true | false]
    redirect-printers [true | false]
    redirect-sound [true | false]
    username-source [session.logon.last.username | none]
    window-height [[integer] | none]
    window-percent-of-desktop [[integer] | none]
    window-size [custom-size | full-screen | percent-of-desktop | seamless]
    window-width [[integer] | none]
    work-dir [[string] | none]
edit rdp [ [ [name] | [glob] | [regex] ] ... ]
    all-properties
    non-default-properties
```

Display

```
list rdp
list rdp [ [ [name] | [glob] | [regex] ] ... ]
show running-config rdp
show running-config rdp [ [ [name] | [glob] | [regex] ] ... ]
    all-properties
    non-default-properties
show rdp
show rdp [name]
```

Delete

```
delete rdp [name]
```

Description

You can use the **rdp** component to configure an MSRDP resource.

Examples

- **create rdp myrdp { host 172.29.67.130 }**
  Creates a MSRDP remote desktop resource named **myrdp** with an MSRDP server with an IP address of **172.29.67.130**.
- **create rdp myrdp { host 172.29.67.130 rdp-cache-bitmaps true }**
  Creates a MSRDP remote desktop resource named **myrdp** with an MSRDP server with an IP address of **172.29.67.130** where bitmaps are cached on the client PC.

Options

- **acl-order**
  Specifies the order in which you want the RDP server to appear in the ACL Order list. The default is **0** (zero).
- **application**
  Specifies the executable name of the application, for example **notepad.exe**. You can include the full path to the application, for example **"C:mymybinary.exe"**.
- **app-service**
  Specifies the name of the application service to which the object belongs. The default value is **none**. **Note:** If the **strict-updates** option is **enabled** on the application service that owns the object, you cannot modify or delete the object. Only the application service can modify or delete the object.

- **auto-logon**
  Specifies if automatic log on to the Microsoft RDP server is used. If you **enable** this option, you must also provide values for the **username-source**, **password-source**, and **domain-source** options. The default is **disabled**.
- **color-depth**
  Specifies the requested remote session color depth. The default is **32**. The options are:
  - **24-bit**
  - **16-bit**
  - **8-bit**
  - **4-bit**
- **customization-group**
  Specifies whether customization-groups are applied to the remote desktop. You can add, modify, delete, or replace all customization-groups. The default is **none**.
- **description**
  Specifies a description of an MSRDP resource. The default is **none**.
- **domain-source**
  Specifies the session variable used as a source for the **auto-logon** user password. The default is **session.logon.last.domain**.
- **host**
  Specifies the hostname of your Microsoft RDP server. Either the **host** or **ip** option is required; however, you cannot specify both options.
- **ip**
  Specifies the IP address of your Microsoft RDP server. Either the **host** or **ip** option is required; however, you cannot specify both options.
- **java-client**
  Specifies if JavaScript is enabled or disabled on the client. The default is **enabled**.
- **location-specific**
  Specifies whether or not this object contains one or more attributes with values that are specific to the location where the BIG-IP device resides. The location-specific attribute is either true or false. When using policy sync, mark an object as location-specific to prevent errors that can occur when policies reference objects, such as authentication servers, that are specific to a certain location.
- **log**
  Specifies the log format. The default is **none**. The options are:
  - **config**

- **none**
  The system does not log packets sent to and from the Microsoft RDP server.
- **packet**
  The system logs packets sent to and from the Microsoft DP server.
- **summary**
  The system provides a short summary of the communications between the BIG-IP system and the Microsoft RDP server.
- **verbose**
  The system provides an extensive summary of the communications between the BIG-IP system and the Microsoft RDP server.

◆ **[name]**
Specifies an object name. This option is required; however, the parameter **name** is implicit and must not be typed in the syntax.

◆ **password-source**
Specifies the session variable used as a source for the **auto-logon** password. The default is **session.logon.last.password**.

◆ **port**
Specify port **3389** for your Microsoft RDP server. The default is **0** (zero).

◆ **rdp-cache-bitmaps**
Specifies whether to cache bitmap files on the client. The default is **true**.

◆ **rdp-show-contents-while-dragging**
Specifies whether to show the contents of a window when the user is dragging the window. The default is **false**.

◆ **rdp-show-desktop-wallpaper**
Specifies whether to display the desktop background. The default is **false**.

◆ **rdp-show-themes**
Specifies whether to display the desktop theme. The default is **false**.

◆ **rdp-window-animations**
Specifies whether to display Window animations. The default is **false**.

◆ **redirect-com-ports**
Specifies whether to connect to your communication ports. The default is **false**.

◆ **redirect-drives**
Specifies whether to connect to your local drives. The default is **false**.

◆ **redirect-keyboard-commands**
Specifies when to redirect keyboard commands to a remote session. When enabled, commands such as **Alt-tab** and **Ctrl-Alt-Del** are available in remote sessions. The default is **in-full-screen**. The options are:

- **enable**
  The keyboard commands for the remote desktop are available to the user.

  - **disable**
    The keyboard commands for the remote desktop are not available to the user.
  - **in-full-screen**
    The keyboard commands for the remote desktop are available to the user only when the value of the **window-size** option is **full-screen**.
- **redirect-printers**
  Enables or disables connection to a local printer. The default is **disabled**.
- **redirect-sound**
  Enables or disables sounds playing in a remote session. The default is **disabled**.
- **username-source**
  Specifies the session variable used as a source for the **auto-logon** user name. The default is **session.logon.last.username**.
- **window-height**
  Specifies the height, in pixels, of the remote desktop window. Set this option only when you set the value of the **window-size** option to **custom**. The default is **600** pixels.
- **window-percent-of-desktop**
  Specifies the width and height of the remote session window as a percentage of the user's desktop.
- **window-size**
  Specifies the type of window sizing to use on the client desktop. The default is **custom-size**.
  The options are:
  - **full-screen**
    The remote desktop window fills the entire screen.
  - **percent-of-desktop**
    The value you configure represents a percentage of the screen that the remote desktop fills.
  - **custom**
    When you use this option, you must also set the **window-height** and **window-width** options.
  - **seamless**
- **window-width**
  Specifies the width, in pixels, of the remote desktop window. The default is **800** pixels.
- **workdir**
  Specifies the directory you want the user to access on the target server. The default is **none**.

See Also

citrix, *citrix-client-bundle*, *citrix-client-package-file*, *vmware-view*, *quest*

vmware-view

Configures a VMware View remote desktop resource configuration object.

Syntax

Configure the **vmware-view** component within the **resource remote desktop** module using the syntax shown in the following sections.

Create/Modify

```
create vmware-view [name]
modify vmware-view [name]
    app-service [[string] | none]
    auto-logon [enabled | disabled]
    customization-group [add | delete | modify | replace-all-with] {
      [name] {
          caption [[string] | none]
          detailed-description [[string] | none]
       }
    }
    description [[string] | none]
    domain-source [session.logon.last.domain | none]
    enable-serverside-ssl [enabled | disabled]
    pool [pool name]
    host [fqdn]
    ip [ip address]
    location-specific [true | false]
    password-source [session.logon.last.password | none]
    port [[string] | none]
    username-source [session.logon.last.username | none]
edit vmware-view [ [ [name] | [glob] | [regex] ] ... ]
    all-properties
    non-default-properties
```

Display

```
list vmware-view
list vmware-view [ [ [name] | [glob] | [regex] ] ... ]
show running-config vmware-view
show running-config vmware-view [ [ [name] | [glob] | [regex] ] ... ]
    all-properties
    non-default-properties
show vmware-view
show vmware-view [name]
```

Delete

```
delete vmware-view [name]
```

Description

You can use the B<vmware-view> component to configure a VMware View remote desktop resource.

Examples

- **create vmware-view myview { ip 172.29.67.130 }**
  Creates a VMware View remote desktop resource named **myview** with the VMware View Connection server specified as IP address **172.29.67.130**.
- **create vmware-view myview { host myview.mycompany.com auto-logon enabled }**
  Creates a VMware View resource with the VMware View Connection server specified as hostname **myview.mycompany.com** and auto-logon enabled with APM credentials (that user types on Logon Page).
- **create vmware-view mview { pool /Common/myview-pool enable-serverside-ssl enabled }**
  Creates a VMware View resource with the VMware View Connection server(s) specified in pool named **/Common/myview-pool** and SSL communication enabled to the server(s) (SSL should also be enabled on the servers and APM virtual should have serverssl profile).

Options

- **app-service**
  Specifies the name of the application service to which the object belongs. The default value is **none**. **Note:** If the **strict-updates** option is **enabled** on the application service that owns the object, you cannot modify or delete the object. Only the application service can modify or delete the object.
- **auto-logon**
  Enables or disables automatic log on to the VMware View Connection Server server. If you enable this option, you must also provide values for the **username-source**, **password-source**, and **domain-source** options. The default is **disabled**.
- **customization-group**
  Specifies whether customization groups are applied to the VMware View resource. You can add, modify, or delete customization groups. You can also replace all current customization groups with new customization groups. The default is **none**.
- **description**
  Specifies a description for your VMware View remote desktop. The default is **none**.
- **domain-source**
  Specifies the Session variable used as a source for the **auto-logon** user password. The default is **session.logon.last.domain**.

- **enable-serverside-ssl**
  Enables or disables SSL capabilities between the BIG-IP system and the VMware View Connection server. When enabled, the port number automatically changes to **443**. The default is **disabled**.
- **pool**
  Specifies the pool name that contains your VMware View Connection server(s). You must use one of these options to specify the server address: **pool**, **host**, or **ip**.
- **host**
  Specifies the hostname of your VMware View Connection server. You must use one of these options to specify the server address: **pool**, **host**, or **ip**.
- **ip**
  Specifies the IP address of your VMware View Connection server. You must use one of these options to specify the server address: **pool**, **host**, or **ip**.
- **location-specific**
  Specifies whether or not this object contains one or more attributes with values that are specific to the location where the BIG-IP device resides. The location-specific attribute is either true or false. When using policy sync, mark an object as location-specific to prevent errors that can occur when policies reference objects, such as authentication servers, that are specific to a certain location.
- **[name]**
  Specifies an object name. This option is required; however, the parameter **name** is implicit and must not be typed in the syntax.
- **password-source**
  Specifies the session variable that is used as a source for the **auto-logon** password. The default is **session.logon.last.password**.
- **port**
  Specifies the port for your VMware View Connection server. The default is **80**.
- **username-source**
  Specifies the session variable that is used as a source for the **auto-logon** user name. The default is **session.logon.last.username**.

See Also

citrix, *rdp*, *quest*

39

apm saml

- Introducing the apm saml module
- Alphabetical list of components

Introducing the apm saml module

You can use the tmsh components that reside within the apm SAML module to configure BIG-IP® Access Policy Manager®. For more information about the tmsh hierarchical structure, see Chapter 2, *Understanding and Using the Traffic Management Shell*.

Alphabetical list of components

The remainder of this chapter lists the tmsh components that are available in the apm SAML module.

artifact-resolution-service

Specify service used to resolve SAML artifacts

Syntax

Configure the **artifact-resolution-service** component within the **saml** module using the syntax shown in the following sections.

Create/Modify

```
create artifact-resolution-service [name]
modify artifact-resolution-service [name]
    app-service [[string] | none]
    artifact-resolution-service-host [[string] | none]
    artifact-resolution-service-port [integer]
    artifact-send-method [http-post | http-redirect]
    artifact-validity [integer]
    basic-auth-password [[string] | none]
    basic-auth-username [[string] | none]
    description [[string] | none]
    location-specific [ true | false ]
    virtual-server-name [name]
    want-artifact-resolution-rq-signed [true | false]
edit artifact-resolution-service [ [ [name] | [glob] | [regex] ] ... ]
    all-properties
    non-default-properties
```

Display

```
list artifact-resolution-service
list artifact-resolution-service [ [ [name] | [glob] | [regex] ] ... ]
show running-config artifact-resolution-service
show running-config artifact-resolution-service [ [ [name] | [glob] | [regex] ] ... ]
    all-properties
    app-service
    non-default-properties
    one-line
    partition
```

Delete

```
delete artifact-resolution-service [name]
```

Description

You can use the **artifact-resolution-service** to create and manage artifact resolution services.

Examples

- **create artifact-resolution-service my_ars {virtual-server-name my_virt}**
  Creates a SAML artifact resolution service named **my_ars**. In this example, the virtual server my_virt will be used to receive artifact resolve requests and send artifact responses.
- **create artifact-resolution-service my_ars1 {virtual-server-name my_virt1 artifact-resolution-service-host bigip.mycompany.com basic-auth-username user basic-auth-password password artifact-send-method http-redirect }**
  Creates a SAML artifact resolution service named **my_ars1**. The service requires that artifact resolve requests be sent using the http-redirect method with an authorization header that contains the specified credentials.
- **list artifact-resolution-service**
  Displays a list of artifact resolution services.
- **delete artifact-resolution-service my_ars**
  Deletes the **my_ars** artifact resolution service.

Options

- **app-service**
  Specifies the name of the application service to which the object belongs. The default value is **none**. **Note:** If the **strict-updates** option is **enabled** on the application service that owns the object, you cannot modify or delete the object. Only the application service can modify or delete the object.
- **artifact-resolution-service-host**
  Specifies the hostname of the artifact resolution service.
- **artifact-resolution-service-port**
  Specifies the port that artifact resolution service will be listening on.
- **artifact-send-method**
  Specifies method resolver will use when sending artifact resolve requests. Default value is **http-redirect**.
- **artifact-validity**
  Specifies in seconds how long an artifact remains valid. Default value is **60** seconds.
- **basic-auth-password**
  Specifies the basic authentication password to send with an artifact resolve request to this BIG-IP.
- **basic-auth-username**
  Specifies the basic authentication username to send with an artifact resolve request to this BIG-IP.
- **description**
  Specifies a unique description for the artifact resolution service. Default is **none**.

- **location-specific**
  Objects of this class might have location-specific attributes. If the object is location-specific, set to true.
- **virtual-server-name**
  Specifies the virtual server to be used by the artifact resolution service.
- **want-artifact-resolution-rq-signed**
  Specifies whether this BIG-IP requires artifact resolve requests to be signed. Default value is true.

40

apm sso

- Introducing the apm sso module
- Alphabetical list of components

Introducing the apm sso module

You can use the tmsh components that reside within the apm sso module to configure BIG-IP® Access Policy Manager®. For more information about the tmsh hierarchical structure, see Chapter 2, *Understanding and Using the Traffic Management Shell*.

Alphabetical list of components

The remainder of this chapter lists the tmsh components that are available in the apm sso module.

basic

Configures a single sign-on HTTP basic authentication configuration object.

Syntax

Configure the **basic** component within the **sso** module using the syntax shown in the following sections.

Create/Modify

```
create basic [name]
modify basic [name]
   app-service [[string] | none]
   headers [add | delete | modify | | replace-all-with] {
   location-specific [true | false]
   [name] {
       app-service [[string] | none]
    hname [[URL] | none]
       hvalue [[integer] | none]
}
   }
password-source [session.sso.token.last.password | none]
       username-conversion [enabled | disabled]
username-source [session.sso.token.last.username | none
```

```
edit basic [ [ [name] | [glob] | [regex] ] ... ]
     all-properties
     non-default-properties
```

Display

```
list basic
list basic [ [ [name] | [glob] | [regex] ] ... ]
show running-config basic
show running-config basic [ [ [name] | [glob] |
                            [regex] ] ... ]
    all-properties
    non-default-properties
    one-line
    partition
```

```
show basic
show basic [name]
```

Delete

```
delete basic [name]
```

Description

You can use the **basic** component to create, modify, display, or delete an SSO HTTP basic authentication configuration object.

Examples

create basic mybasic

Creates an SSO **basic** configuration object named **mybasic**.

Options

- **app-service**
  Specifies the name of the application service to which the object belongs. The default value is **none**. **Note:** If the **strict-updates** option is **enabled** on the application service that owns the object, you cannot modify or delete the object. Only the application service can modify or delete the object.
- **headers**
  Specifies the name and value of the HTTP header content to be inserted in an HTTP Request that passes through the APM SSO module. The default is **none**. The options are:
  - **app-service**
    Specifies the name of the application service to which the HTTP header belongs. The default value is **none**. **Note:** If the **strict-updates** option is **enabled** on the application service that owns the object, you cannot modify or delete the HTTP header. Only the application service can modify or delete the HTTP header.
  - **hname**
    The name of the HTTP header.
  - **hvalue**
    The value of the HTTP header.
- **location-specific**
  Specifies whether or not this object contains one or more attributes with values that are specific to the location where the BIG-IP device resides. The location-specific attribute is either true or false. When using policy sync, mark an object as location-specific to prevent errors that can occur when policies reference objects, such as authentication servers, that are specific to a certain location.
- **[name]**
  Specifies a name for the SSO configuration. This option is required.
- **partition**
  Displays the partition in which the object resides.
- **oam-server**
  Specifies the name of your Oracle Access Manager server. The default value is **none**.
- **password source**
  Specifies the source from which you want SSO to retrieve the password to use to authenticate applications.
- **username-conversion**
  Enables or disables conversion of PREWIN2k/UPN username input format to the format for SSO to use. The default value is **disabled**.

- **username-source**
  Specifies the source from which you want SSO to retrieve the username to use to authenticate applications.

form-based

Configures a single sign-on form-based configuration object.

Syntax

Configure the **form-based** component within the **sso** module using the syntax shown in the following sections.

Create/Modify

```
create form-based [name]
modify form-based [name]
    app-service [[string] | none]
    external-access-management [oam | none]
    form-action [[URL] | none]
    form-field [string]
    form-method [get | post]
    form-password [string]
    form-username [string]
    headers [add | delete | modify | | replace-all-with] {
      [name] {
          app-service [[string] | none]
       hname [[URL] | none]
          hvalue [[integer] | none]
  }
    }
    password-source [session.sso.token.last.password | none]
    start-uri [[URLs] | none]
    success-match-type [cookie | none | url]
    success-match-value [string]
    username-source [session.sso.token.last.username | none
edit form-based [ [ [name] | [glob] | [regex] ] ... ]
    all-properties
    non-default-properties
```

Display

```
list form-based
list form-based [ [ [name] | [glob] | [regex] ] ... ]
show running-config form-based
show running-config form-based [ [ [name] | [glob] |
                            [regex] ] ... ]
    all-properties
    non-default-properties
    one-line
    partition
show form-based
show form-based [name]
```

Delete

```
delete form-based [name]
```

Description

You can use the **form-based** component to configure an SSO form-based configuration object.

Examples

create form-based fb_2011_sso { start-uri "/fb/auth/logon.aspxurl=https://exch2011.mv1.fp.com/fp/&reason=0" form-action "/fp/auth/fpauth.dll" form-username "username" form-password "password" form-field "destination https://exch2011.mv1.fp.com/fp/" }

Creates an SSO **form-based** configuration object named **fb_2011_sso**.

Options

- **app-service**
  Specifies the name of the application service to which the object belongs. The default value is **none**. **Note:** If the **strict-updates** option is **enabled** on the application service that owns the object, you cannot modify or delete the object. Only the application service can modify or delete the object.
- **external-access-management**
- **form-action**
  Specifies the form action URL that is used for HTTP form-based authentication. This is optional. If you do not specify a form action, then Access Policy Manager uses the URI from the request to perform HTTP form-based authentication. The default is **none**.
- **form-field**
  Specifies the hidden form parameters that are required by the authentication server logon form at your location. Refer to the *BIG-IP® Configuration Guide: Access Policy Manager®* for more information on how to determine hidden values. The default is **none**.
- **form-method**
  Specifies the form method to use for form-based HTTP authentication. The value is either **get** or **post**. The default is **post**.
  If you specify **get**, Access Policy Manager forces the authentication using HTTP GET rather than authenticating using form-based POST.
- **form-password**
  Specifies the parameter names used by the form that is sent the POST request.
- **form-username**
  Specifies the parameter names used by the form that is sent the POST request.

- **headers**
  Specifies the name and value of the HTTP header content to be inserted in an HTTP Request that passes through the APM SSO module. The default is **none**.
  The options are:
  - **app-service**
    Specifies the name of the application service to which the HTTP header belongs. The default value is **none**. **Note:** If the **strict-updates** option is **enabled** on the application service that owns the object, you cannot modify or delete the HTTP header. Only the application service can modify or delete the HTTP header.
  - **hname**
    Specifies the name of the HTTP header.
  - **hvalue**
    Specifies the value of the HTTP header.
- **[name]**
  Specifies a name for the component.
- **password-source**
  Specifies the password you want cached for single sign-on.
  The default is **session.sso.token.last.password**.
- **start-uri**
  Specifies a URL resource. For example, for FB, it would be **/fb/auth/logon.aspx***. For Citrix, **/Citrix/XenApp/auth/logon.aspx**. This resource must respond with a challenge to a non-authenticated request.
  The default is **none**.
- **success-match-type**
  Specifies the method your authentication server uses. If you specify a value for this option, you must also specify a value for **success-match-value**. The default is **none**. The options are:
  - **url**
    One or more URLs. The system supports only the wildcard character (*).
  - **cookie**
    A cookie name.
- **success-match-value**
  Specifies the value used to specify either the URL(s) or cookie for the **success-match-type** option. The default is **none**.
- **username-source**
  Specify the username you want cached for single sign-on. The default is **session.sso.token.last.username**.

See Also

basic, *kerberos*, *ntlmv1*, *ntlmv2*

form-basedv2

Configures a single sign-on form-basedv2 configuration object.

Syntax

Configure the **form-basedv2** component within the **sso** module using the syntax shown in the following sections.

Create/Modify

```
create form-basedv2 [name]
    app-service [[string] | none]
    forms [add | replace-all-with] {
      [name] {
        request-value [URIs]
        controls [add | replace-all-with] {
          [name] {
            value [string]
          }
        }
      }
    }
modify form-basedv2 [name]
    app-service [[string] | none]
    forms [add | delete | modify | replace-all-with] {
      [name] {
          app-service [[string] | none]
          attribute-value [[string] | none]
          controls [add | delete | modify | replace-all-with] {
            [name] {
                app-service [[string] | none]
                secure [true | false]
                value [string]
            }
          }
          description [[string] | none]
          form-order [integer]
          id-type [action | id | inputs | name | order]
          request-method [get | post]
          request-name [[string] | none]
          request-negative [true | false]
          request-prefix [true | false]
          request-type [cookie | header | uri]
          request-value [[string] | none]
          submit-autodetect [true | false]
          submit-javascript [[string] | none]
          submit-javascript-type [auto | custom | extra]
          submit-method post
          submit-name [[string] | none]
          submit-negative [true | false]
          submit-prefix [true | false]
          submit-type [cookie | header | uri]
          submit-value [[string] | none]
          success-match-type [cookie | none | url]
          success-match-value [[string] | none]
      }
```

```
    }
    headers [add | delete | modify | none | replace-all-with] {
      [name] {
          app-service [[string] | none]
          description [[string] | none]
          name [string]
          value [string]
      }
    }
    log-level [alert | crit | debug | emerg | err | info | notice | warn]
edit form-basedv2 [ [ [name] | [glob] | [regex] ] ... ]
    all-properties
    non-default-properties
reset-stats
reset-stats [ [ [name] | [glob] | [regex] ] ... ]
```

Display

```
list form-basedv2
list form-basedv2 [ [ [name] | [glob] | [regex] ] ... ]
show running-config form-basedv2
show running-config form-basedv2 [ [ [name] | [glob] |
                          [regex] ] ... ]
    all-properties
    non-default-properties
    one-line
    partition
show form-basedv2
show form-basedv2 [name]
```

Delete

```
delete form-basedv2 [name]
```

Description

You can use the **form-basedv2** component to configure an SSO form-basedv2 configuration object. When creating a new SSO form-based v2 configuration object, you must add at least one **forms** item and within it at least one **controls** item. You must also provide a value for the **request-value** option in the **forms** item.

The SSOv2 module identifies and processes two types of application HTTP requests - logon page requests and credentials submit requests. Logon page requests are identified using the **request-** set of options. Credentials submit requests, in most cases, are identified automatically. When this fails, you can set the **submit-autodetect** option to **false** and use the **submit-** set of options to identify these requests.

When the SSOv2 module identifies a logon page request, it scans the response trying to find the logon form. If the logon form is found, SSOv2 inserts a JavaScript code that will cause the logon form to be submitted automatically by the browser. The client must support JavaScript.

When the SSOv2 module identifies a credentials submit request, it compares POST data parameter names with form controls defined in the configuration. For a POST data parameter name that has a corresponding form control, the SSOv2 module replaces its value with the control value from the configuration. Control values are usually supplied through session variables, such as session.sso.token.last.username and session.sso.token.last.password. POST data parameters that have no corresponding controls in the configuration are not changed.

The majority of web applications have a single logon page with one logon form. You will need to define a single **forms** item for these applications. In rare cases when an application has multiple logon pages with different logon forms, you will need to create multiple **forms** items, one for each logon page/form. If multiple logon pages use the same form, you will need only one **forms** item with a list of URIs for all logon pages.

Every **forms** item must include at least one **controls** item, and can include up to 32 **controls** items. Each **controls** item represents an input element of an HTML logon form, such as form fields for entering username and password, and, optionally, any hidden form parameters. The name of the **controls** item must match the name attribute of the corresponding input tag of the form. For example, if the form has the following HTML tag for entering the username:

```
<input id="Bugzilla_login_top"
       class="bz_login"
       name="Bugzilla_login"
       onfocus="mini_login_on_focus('_top')"
>
```

the **forms** item must include a **controls** item with the name **Bugzilla_login**. The **controls** item used for entering the user's password must have the **secure** option set to **true**. The value of a control item should usually be the name of a session variable, starting with the percent (%) sign and enclosed in curly braces ({}); for example, the value for the username control item: %{session.sso.token.last.username}. The value can also be a string, or a combination of strings and session variable names.

Examples

create form-basedv2 fbssov2-owa2010 { forms add { owa2010 { controls add { password { secure true value %{session.sso.token.last.password} } username { value %{session.sso.token.last.username} } } request-value /owa/auth/logon.aspx?replaceCurrent=1 submit-javascript clkLgn() submit-javascript-type extra success-match-type cookie success-match-value sessionid } } }

Creates an SSO **form-basedv2** configuration object named **fbssov2-owa2010**.

delete fbsso-owa2010

Deletes an SSO **form-basedv2** configuration object named **fbssov2-owa2010**.

Options

- **app-service**
  Specifies the name of the application service to which the object belongs. The default value is **none**. **Note:** If the **strict-updates** option is **enabled** on the application service that owns the object, you cannot modify or delete the object. Only the application service can modify or delete the object.
- **forms**
  Specifies one or more items, each defining SSO processing of a separate application logon form.
- **[name]**
  Specifies the name of the form item. It does not have to match the actual name of the HTML form and can be arbitrary.
  The options are:
  - **app-service**
    Specifies the name of the application service to which the form item belongs. The default value is **none**. **Note:** If the **strict-updates** option is **enabled** on the application service that owns the object, you cannot modify or delete the form item. Only the application service can modify or delete the form item.
  - **attribute-value**
    Specifies the value of the HTML <form> tag attribute used to identify the logon form. The attribute could be **id**, **name**, or **action**, and is specified by the **id-type** option. For other values of the **id-type** option, this is not used and should be set to **none**.
  - **controls**
    Specifies one or more form control items (up to 32) that you want to be processed by SSOv2.
- **[name]**
  Specifies the name of the HTML form control item. It must match the name attribute value of the HTML form's input tag.
  The options are:
  - **app-service**
    Specifies the name of the application service to which the control item belongs. The default value is **none**. **Note:** If the **strict-updates** option is **enabled** on the application service that owns the object, you cannot modify or delete the control item. Only the application service can modify or delete the control item.
  - **secure**
    Specifies whether the control item represents the HTML input tag of type "password". The default is **false**.
  - **value**
    Specifies the value of the control item. This is usually the name of a session variable. If the session variable is not found when the SSO request is processed, the value of the corresponding POST parameter will be empty. The value could also be a literal string or a combination of strings and session variable names.

- **description**
  User-defined description.
- **form-order**
  Specifies the order of the HTML logon form on the logon page when the **id-type** option is set to **order**. Starts with 1.
- **id-type**
  Specifies how the HTML logon form is found in the HTML body of the logon page. If there is more than one form on the logon page matching the criteria, the first match is used. The default is **inputs**.
  The options are:
  - **action**
    The logon form is identified by the value of the <form> tag in the **action** attribute. The value is specified in the **attribute-value** option.
  - **id**
    The logon form is identified by the **id** attribute's value of the <form> tag. The value is specified in the **attribute-value** option.
  - **name**
    The logon form is identified by the **name** attribute's value of the <form> tag. The value is specified in the **attribute-value** option.
  - **order**
    The logon form is identified by its relative order on the logon page (starting from 1). The order is specified in the **form-order** option.
  - **inputs**
    The logon form is identified by a combination of **controls** items. The controls in the configuration must have corresponding <input> elements in the form.
- **request-method**
  Specifies the HTTP method of the application's request returning logon page. Default is **get**.
- **request-name**
  Specifies the name of the HTTP cookie or the name of the HTTP header used to identify application's request for logon page. The cookie or header is selected by the **request-type** option. The value of the cookie or header is specified by the **request-value** option. When the **request-type** option is set to **uri**, this option is not used and should be set to **none**.
- **request-negative**
  When set to **true**, the application's request for logon page will be identified by the absence of the specified cookie or header, or by a failed match against the list of specified URIs. The default is **false**.
- **request-prefix**
  Specifies how the value of the **request-value** option will be used to match one of the HTTP request cookie, header, or URI. The default is **true** and specifies a partial match; **false** specifies an exact match.
- **request-type**
  Specifies which element of the HTTP request headers is used to identify the application's request for logon page. The default is **uri**.
  The options are:

- **cookie**
  The request is identified by the presence (or absence) of a cookie. The name and value of the cookie are specified by the **request-name** and **request-value** options.
- **header**
  The request is identified by the presence (or absence) of the HTTP header. The name and value of the header are specified by the **request-name** and **request-value** options.
- **uri**
  The request is identified by a successful (or failed) match against a list of URIs specified by the **request-value** option, and the **request-name** option is not used.

◆ **request-value**
Specifies the value of the HTTP request element that must be matched to identify the request as the application's request for the logon page. This is one of: the cookie value, the header value, or a list of URIs (one per line) as specified by the **request-type** option. Cookie or header value could be set to **none**, in which case only the presence of the named cookie or header is checked and the value is not checked. When checking for URI, the value must be specified.

◆ **submit-autodetect**
When set to **true**, the application's HTTP request that submits the user's credentials will be identified automatically and other **submit-** options should not be used. When **false**, the form submit will be identified using a combination of other **submit-** options. The default is **true**.

◆ **submit-javascript**
Specifies user-provided JavaScript code to be inserted into the logon page to perform automatic form submission when the **submit-javascript-type** option is set to **custom**. The custom JavaScript code replaces the code automatically generated by the SSOv2 module. When the **submit-javascript-type** option is set to **extra**, it specifies the application's JavaScript functions to call from the automatically generated JavaScript code prior to submitting a logon form. When the **submit-javascript-type** option is set to **auto**, this option should be set to **none**.

◆ **submit-javascript-type**
Specifies the type of JavaScript code to be inserted into the logon page by the SSOv2 module to perform automatic logon form submission. The options are:

- **auto**
  JavaScript code is automatically generated by the SSOv2 module.
- **custom**
  JavaScript code is provided by the user in the **submit-javascript** option.

- **extra**
  JavaScript code is automatically generated by the SSOv2 module, and additional JavaScript code provided by the user in the **submit-javascript** option is inserted before the form submit statement.

- **submit-method**
  Specifies the HTTP method of credentials submit request for the application. This must be set to **post**. This option is not used when **submit-autodetect** is true.
- **submit-name**
  Specifies the name of the HTTP cookie or the name of HTTP header used to identify credentials submit request for the application. The cookie or header is selected by the **submit-type** option. The value of the cookie or header is specified by the **submit-value** option. When the **submit-type** option is set to **uri**, this option is not used and should be set to **none**. This option is not used when **submit-autodetect** is true.
- **submit-negative**
  When set to **true**, the credentials submit request for the application is identified by the absence of a specified cookie or header, or by a failed match against the list of specified URIs. The default is **false**. This option is not used when **submit-autodetect** is true.
- **submit-prefix**
  Specifies how the value of the **submit-value** option will be used to match the HTTP request cookie, header, or URI. The default is **true** and specifies partial match; **false** specifies exact match. This option is not used when **submit-autodetect** is true.
- **submit-type**
  Specifies which element of HTTP request headers is used to identify the credentials submit request for the application. The default is **uri**. This option is not used when **submit-autodetect** is true.
  The options are:

  - **cookie**
    The request is identified by the presence (or absence) of a cookie. The name and value of the cookie are specified by the **submit-name** and **submit-value** options.
  - **header**
    The request is identified by the presence (or absence) of the HTTP header. The name and value of the header are specified by the **submit-name** and **submit-value** options.
  - **uri**
    The request is identified by a successful (or failed) match against a list of URIs specified by the **submit-value** option and the **submit-name** option is not used.
- **submit-value**
  Specifies the value of the HTTP request element that must be matched to identify the request as a credentials submit request for the application. This is one of: the cookie value, the header value, or a list of URIs (one per line) as specified by the **submit-type** option. Cookie or header value

could be set to **none**, in which case only the presence of the named cookie or header is checked and the value is not checked. When checking for URI, the value must be specified. This option is not used when **submit-autodetect** is true.

- **success-match-type**
  Specifies how the SSOv2 module detects whether the credentials submit request was successful. When the SSOv2 module detects that the credentials submission failed, the SSOv2 configuration used for this HTTP transaction is disabled for the user session. If you specify a value for this option, you must also specify a value for **success-match-value**. The default is **none**. The options are:
  - **url**
    Credentials submission was successful if the response contains the HTTP Location header with a value matching one of the URLs specified by the **success-match-value** option.
  - **cookie**
    Credentials submission was successful if the response contains the HTTP cookie with the name specified by the **success-match-value** option.
  - **none**
    No check is performed. If SSO logon fails and the application server redirects back to the logon page that matches the criteria of the logon page request, SSO will be retried, possibly causing authentication loop.
- **success-match-value**
  Specifies the value used to detect the success or failure of the SSO logon. When the **success-match-type** option is set to **url**, this is a list of URLs. Each URL in the list can contain a single wildcard character (*). When the **success-match-type** option is set to **cookie**, this option specifies the name of the cookie. The default is **none**.
- **headers**
  Specifies the name and value of the HTTP header to be inserted in an HTTP Request that passes through the APM SSOv2 module.
- **[name]**
  Specifies the name of the headers item.
  The options are:
  - **app-service**
    Specifies the name of the application service to which the HTTP header belongs. The default value is **none**. **Note:** If the **strict-updates** option is **enabled** on the application service that owns the object, you cannot modify or delete the HTTP header. Only the application service can modify or delete the HTTP header.
  - **name**
    Specifies the name of the HTTP header.
  - **value**
    Specifies the value of the HTTP header.

- **log-level**
  Specifies the log level. Valid values are **alert**, **crit**, **debug**, **emerg**, **err**, **info**, **notice**, **warn**. The default is **notice**.

See Also

basic, *kerberos*, *ntlmv1*, *ntlmv2*, *form-based*

kerberos

Configures a Kerberos configuration object.

Syntax

Configure the **kerberos** component within the **sso** module using the syntax shown in the following sections.

Create/Modify

```
create kerberos [name]
modify kerberos [name]
    account-name [string]
    account-password [string]
    app-service [[string] | none]
    headers [add | delete | modify | replace-all-with] {
      [name] {
          app-service [[string] | none]
          hname [[string] | none]
          hvalue [[integer] | none]
       }
    }
    kdc [[string] | none]
    location-specific [true | false]
    realm [string]
    send-authorization [401 | always]
    spn-pattern [[string] | none]
    ticket-lifetime [[integer] | none]
edit kerberos [ [ [name] | [glob] | [regex] ] ... ]
    all-properties
    non-default-properties
```

Display

```
list kerberos
list kerberos [ [ [name] | [glob] | [regex] ] ... ]
show running-config kerberos
show running-config kerberos [ [ [name] | [glob] | [regex] ] ... ]
    all-properties
    non-default-properties
    one-line
    partition
show kerberos
show kerberos [name]
```

Delete

```
delete kerberos [name]
```

Description

You can use the **kerberos** component to configure an SSO Kerberos configuration object. Kerberos is an authentication protocol, where both the user and the server verify the other's identity.

Examples

- **create mykerberos { realm MYREALM.COM account-name apmaccount account-password **** }**
  Creates an SSO **kerberos** configuration object named **mykerberos** for the realm **myrealm.com**, where the account name is **apmaccount** and the password is ****.

Options

- **account-name**
  Specifies the name of the Active Directory account configured for delegation. This account must be configured in the server's Kerberos realm (AD Domain). If servers are from multiple realms, each realm (AD Domain) must have its own delegation account. This option is required.
- **account-password**
  Specifies the password for the delegation account specified in **account-name**. This option is required.
- **app-service**
  Specifies the name of the application service to which the object belongs. The default value is **none**. **Note:** If the **strict-updates** option is **enabled** on the application service that owns the object, you cannot modify or delete the object. Only the application service can modify or delete the object.
- **headers**
  Specifies custom HTTP headers to insert into a request. The default value is **none**. The options are:
  - **app-service**
    Specifies the name of the application service to which the header belongs. The default value is **none**. **Note:** If the **strict-updates** option is **enabled** on the application service that owns the object, you cannot modify or delete the header. Only the application service can modify or delete the header.
  - **hname**
    Specifies the name of a header to add to a request.
  - **hvalue**
    Specifies the value of a header to add to a request.
- **kdc**
  Specifies the IP Address or host name of the Kerberos Key Distribution Center (KDC) for the server's realm. This is normally an Active Directory domain controller. If you leave this empty, the KDC must be

discoverable through DNS, for example, BIG-IP system must be able to fetch SRV records for the server realm's domain. If the server realm's domain name is different from the server's realm name, you must specify the server realm's domain name in the **/etc/krb5.conf** file. Kerberos SSO processing is fastest when KDC is specified by its IP address, slower when specified by host name, and even slower (due to additional DNS queries) when left empty. When a user's realm is different from server's realm, the KDC value must be empty. This is true in cases of cross-realm SSO. The default is **none**.

- **location-specific**
  Specifies whether or not this object contains one or more attributes with values that are specific to the location where the BIG-IP device resides. The location-specific attribute is either true or false. When using policy sync, mark an object as location-specific to prevent errors that can occur when policies reference objects, such as authentication servers, that are specific to a certain location.
- **[name]**
  Specifies the name for the SSO Kerberos configuration object. This option is required.
- **realm**
  Specifies the realm of application server(s), for example, pool members or portal access resource hosts. If the servers are located in multiple realms, each realm requires a separate SSO configuration. You must specify the realm in uppercase letters. The user's realm can be specified through the **session.logon.last.domain** session variable, and if this variable is not set, then the user's realm is assumed to be the same as the server's realm. This option is required.
- **send-authorization**
  Specifies when to submit a Kerberos ticket to the application server(s). The ticket is submitted in an HTTP Authorization header. The header value starts with the word **Negotiate**, followed by one space and a base64-encoded GSSIAPI token containing the Kerberos ticket. If a request contains an Authorization header from the user's browser, it is deleted. The default is **always**. The options are:
  - **401**
    The BIG-IP system first forwards the user's HTTP request to the web server without inserting a new Authorization header; however, the browser's Authorization header is deleted. If the server requests authentication by responding with a 401 status code, BIG-IP retries the request with the Authorization header. The Kerberos ticket GSSAPI representation uses the SPNEGO mechanism type (OID 1.3.6.1.5.5.2).
    Specifying **401** results in additional BIG-IP/server request round trips in case authentication is required for the request.
  - **always**
    The BIG-IP system inserts an Authorization header, including the Kerberos ticket, into every HTTP request, whether the request requires authentication or not. The Kerberos ticket GSSAPI representation uses the KRB5 Kerberos 5 mechanism type (OID

1.2.840.113554.1.2.2).
Specifying **Always** results in the additional overhead of generating a Kerberos token for every request. This is the default value.

- **spn-pattern**
Specifies how the Service Principal Name (SPN) for the server is constructed. For example, **HTTP/%s@[server realm name configured in the realm option]**, where **%s** will be substituted with the hostname of your server discovered through reverse DNS lookup using the server IP address. Only specify this option when you need non-standard SPN format. The default is **none**.
- **ticket-lifetime**
Specifies the lifetime of Kerberos tickets obtained for the user. The value represents the maximum ticket lifetime. The actual ticket lifetime may be less by up to 1 hour, because a user's ticket lifetime is the same as the Kerberos Ticket Granting Ticket (TGT) lifetime. A TGT is obtained for the delegation account specified in this configuration. A new TGT is fetched every time the current TGT is older than one hour. The new TGT can only be fetched when an SSO request is processed.
The minimum ticket lifetime is **10** minutes. There is no maximum, however, the ticket lifetime of most AD domains is 10 hours (600 minutes). F5 Networks recommends that you set the ticket lifetime in an SSO configuration above what is specified in an AD domain. The default is **600** minutes.

See Also

basic, *form-based*, *ntlmv1*, *ntlmv2*

ntlmv1

Configures a single sign-on (SSO) NT LAN Manager, version 1 (ntlmv1) configuration object.

Syntax

Configure the **ntlmv1** component within the **sso** module using the syntax shown in the following sections.

Create/Modify

```
create ntlmv1 [name]
modify ntlmv1 [name]
    app-service [[string] | none]
    domain-source [session.logon.last.domain | none]
    headers [add | delete | modify | replace-all-with] {
      [name] {
          app-service [[string] | none]
          hname [[string] | none]
          hvalue [[integer] | none]
       }
    }
    location-specific [true | false]
    ntlm-domain [[string] | none]
    password-source [session.sso.token.last.password | none]
    username-conversion [enabled | disabled]
    username-source [session.sso.token.last.username | none]
edit ntlmv1 [ [ [name] | [glob] | [regex] ] ... ]
    all-properties
    non-default-properties
```

Display

```
list ntlmv1
list ntlmv1 [ [ [name] | [glob] | [regex] ] ... ]
show running-config ntlmv1
show running-config ntlmv1 [ [ [name] | [glob] |
                             [regex] ] ... ]
    all-properties
    non-default-properties
    one-line
    partition
show ntlmv1
show ntlmv1 [name]
```

Delete

```
delete ntlmv1 [name]
```

Description

You can use this **ntlmv1** component to configure a single sign-on NT LAN Manager, version 1 configuration object.

Examples

- **create ntlmv1 myntlmv1**
  Creates an SSO **ntlmv1** configuration object named **myntlmv1**.

Options

- **app-service**
  Specifies the name of the application service to which the object belongs. The default value is **none**. **Note:** If the **strict-updates** option is **enabled** on the application service that owns the object, you cannot modify or delete the object. Only the application service can modify or delete the object.
- **domain-source**
  Specifies the Session variable used as a source for the single sign-on user domain. The default is **session.logon.last.domain**.
- **headers**
  Specifies the name and value of the HTTP header content to be inserted in an HTTP Request that passes through the APM SSO module. The default is **none**.
  The options are:
  - **app-service**
    Specifies the name of the application service to which the HTTP header belongs. The default value is **none**. **Note:** If the **strict-updates** option is **enabled** on the application service that owns the object, you cannot modify or delete the HTTP header. Only the application service can modify or delete the HTTP header.
  - **hname**
    Specifies the name of the HTTP header.
  - **hvalue**
    Specifies the value of the HTTP header.
- **location-specific**
  Specifies whether or not this object contains one or more attributes with values that are specific to the location where the BIG-IP device resides. The location-specific attribute is either true or false. When using policy sync, mark an object as location-specific to prevent errors that can occur when policies reference objects, such as authentication servers, that are specific to a certain location.
- **[name]**
  Specifies the name for the SSO ntlmv1 configuration object. This option is required.

- **ntlm-domain**
  Specifies the static domain setting. If the domain is not retrieved successfully from the source specified in the **domain-source** option, the system uses this value for the source.
- **password source**
  Specifies the source from which you want SSO to retrieve the password to use to authenticate applications. The default is **session.sso.token.last.password**.
- **username-conversion**
  Enables or disables conversion of PREWIN2k/UPN username input format to the format you want to use for SSO. The default is **disabled**.
- **username-source**
  Specifies the source from which you want SSO to retrieve the username used to authenticate applications.

See Also

basic, *form-based*, *kerberos*, *ntlmv2*

ntlmv2

Configures a single sign-on (SSO) NT LAN Manager, version 2 (ntlmv2) configuration object.

Syntax

Configure the **ntlmv2** component within the **sso** module using the syntax shown in the following sections.

Create/Modify

```
create ntlmv2 [name]
modify ntlmv2 [name]
    app-service [[string] | none]
    domain-source [session.logon.last.domain | none]
    headers [add | delete | modify | replace-all-with] {
      [name] {
          app-service [[string] | none]
          hname [[string] | none]
          hvalue [[integer] | none]
       }
    }
    location-specific [true | false]
    ntlm-domain [[string] | none]
    password-source [session.sso.token.last.password | none]
    username-conversion [enabled | disabled]
    username-source [session.sso.token.last.username | none]
edit ntlmv2 [ [ [name] | [glob] | [regex] ] ... ]
    all-properties
    non-default-properties
```

Display

```
list ntlmv2
list ntlmv2 [ [ [name] | [glob] | [regex] ] ... ]
show running-config ntlmv2
show running-config ntlmv2 [ [ [name] | [glob] |
                             [regex] ] ... ]
    all-properties
    non-default-properties
    one-line
    partition
show ntlmv2
show ntlmv2 [name]
```

Delete

```
delete ntlmv2 [name]
```

Description

You can use the **ntlmv2** component to configure a single sign-on NT LAN Manager, version 2 configuration object.

Examples

- **create ntlmv2 myntlmv2**
  Creates an SSO **ntlmv2** configuration object named **myntlmv2**.

Options

- **app-service**
  Specifies the name of the application service to which the object belongs. The default value is **none**. **Note:** If the **strict-updates** option is **enabled** on the application service that owns the object, you cannot modify or delete the object. Only the application service can modify or delete the object.
- **domain-source**
  Specifies the Session variable used as a source for the single sign-on user domain. The default is **session.logon.last.domain**.
- **headers**
  Specifies the name and value of the HTTP header content to be inserted in an HTTP Request that passes through the APM SSO module. The default is **none**.
  The options are:
  - **app-service**
    Specifies the name of the application service to which the HTTP header belongs. The default value is **none**. **Note:** If the **strict-updates** option is **enabled** on the application service that owns the object, you cannot modify or delete the HTTP header. Only the application service can modify or delete the HTTP header.
  - **hname**
    Specifies the name of the HTTP header.
  - **hvalue**
    Specifies the value of the HTTP header.
- **location-specific**
  Specifies whether or not this object contains one or more attributes with values that are specific to the location where the BIG-IP device resides. The location-specific attribute is either true or false. When using policy sync, mark an object as location-specific to prevent errors that can occur when policies reference objects, such as authentication servers, that are specific to a certain location.
- **[name]**
  Specifies a name for the sso ntlmv2 configuration object. This option is required.

- **ntlm-domain**
  Specifies the static domain setting. If the domain is not retrieved successfully from the source specified in the **domain-source** option, the system uses this value for the source.
- **password source**
  Specifies the source from which you want SSO to retrieve the password to use to authenticate applications. The default is **session.sso.token.last.password**.
- **username-conversion**
  Enables or disables conversion of PREWIN2k/UPN username input format to the format you want to use for SSO. The default is **disabled**.
- **username-source**
  Specifies the source from which you want SSO to retrieve the username used to authenticate applications.

See Also

basic, *form-based*, *kerberos*, *ntlmv1*

saml

Specify SAML SSO configuration.

Syntax

Configure the **saml** within the **sso** module using the syntax shown in the following sections.

Create/Modify

```
create saml [name]
modify saml [name]
    app-service [[string] | none]
    artifact-resolution-service-name [name | none]
    assertion-validity [integer]
    attributes [none | {
     {
       name [[string] | none],
       value [[string] | none]
     }
    } ]
    description [[string] | none]
    entity-id [string]
    export-metadata [no-signing | with-signing]
    idp-certificate [string | none]
    idp-signkey [string | none]
    log-level [alert | crit | debug | emerg | err | info | notice | warn]
    location-specific [true | false]
    metadata-cert [[string] | none]
    metadata-file [[string] | none]
    metadata-signkey [string | none]
    sp-connectors [add | delete | modify | none | replace-all-with] {
       [string]
    }
    subject-type [email-address | kerberos | transient | win-domain-qualified-name |
entity | persistent | unspecified | x509-subject]
    subject-value [ string | none ]
edit saml [ [ [name] | [glob] | [regex] ] ... ]
    all-properties
    non-default-properties
```

Display

```
list saml
list saml [ [ [name] | [glob] | [regex] ] ... ]
show running-config saml
show running-config saml [ [ [name] | [glob] | [regex] ] ... ]
    all-properties
    app-service
    non-default-properties
    one-line
    partition
```

Delete

```
delete saml [name]
```

Description

You can use the **saml** component to create and manage SAML SSO objects.

Examples

- **create saml my_saml_sso_obj { entity-id "https://myidpvs.big-ip.com/idp" subject-type email-address subject-value test@mycompany.com idp-certificate default.crt idp-signkey default.key sp-connectors add { google_apps salesforce }}**
  Creates a SAML SSO object named **my_saml_sso_obj** with SP connectors "google_apps" and "salesforce"
- **create saml my_saml_sso_obj1 { entity-id "https://myidpvs.big-ip.com/idp" subject-type email-address subject-value test@mycompany.com idp-certificate default.crt idp-signkey default.key sp-connectors add { google_apps sp_salesforce } attributes {{name "group" value "PD"} {name "title" value "engineer1"}} }**
  Creates a SAML SSO object named **my_saml_sso_obj1** with attributes "group" and "title".
- **list saml**
  Displays list of SAML SSO objects.
- **delete saml my_saml_sso_obj**
  Deletes the **my_saml_sso_obj** SAML SSO object.

Options

- **app-service**
  Specifies the name of the application service to which the object belongs. The default value is **none**. **Note:** If the **strict-updates** option is **enabled** on the application service that owns the object, you cannot modify or delete the object. Only the application service can modify or delete the object.
- **assertion-validity**
  Specifies assertion validity period in seconds.
- **artifact-resolution-service-name**
  Specifies the artifact resolution service to be used by this BIG-IP as IdP to receive artifacts and resolve them for assertions.
- **attributes**
  Specifies list of attributes as part of assertion. Both attribute name and value can be session variables. Configuration "multi-values" is reserved

for future versions and is currently not used.
create saml my_saml_sso_obj1 { entity-id "https://myidpvs.big-ip.com/idp" subject-type email-address subject-value test@mycompany.com idp-certificate default.crt idp-signkey default.key sp-connectors add { google_apps sp_salesforce } attributes {{name "group" value "%{session.ldap.last.attr.primarygroup}"} {name "title" value "engineer1"}} }
Creates a SAML SSO object named **my_saml_sso_obj1** with attributes "group" and "title".

- **description**
  Specifies a unique description for SAML SSO object. The default is **none**.
- **entity-id**
  Specifies unique identifier for IdP that is a URI that points to the BIG-IP virtual server which is going to act as a SAML IdP. For example, if you type "https://mycompany-idp", then "https://mycompany-idp" points to the virtual server you use for APM as a SAML IdP.
- **export-metadata**
  You can simplify SAML configuration using metadata files. When you use APM as an IdP, you can export metadata for IdP. You can save metadata to a file and give it to the SP to enable SP to import SP's SAML configuration or enable SP to use information from the metadata file to configure the IdP. You can choose to sign metadata while exporting it for better security.
  For example:
  1. Exporting metadata with signing. This requires metadata-signkey and metadata-cert files.
  ```
  modify saml my_saml_sso_obj {export-metadata
  with-signing metadata-file
  /shared/idp_signed_metadata.xml metadata-cert
  default.crt metadata-signkey default.key}
  ```

  2. Exporting metadata with no signing.
  ```
  modify saml my_saml_sso_obj {export-metadata
  no-signing metadata-file /shared/idp_metadata.xml}
  ```

- **idp-certificate**
  BIG-IP includes this certificate in the SAML IdP metadata that you export. After the SAML IdP metadata is imported on the SP, the SP can use this certificate to verify the signature of assertion sent by this BIG-IP as IdP.
- **idp-signkey**
  Specifies the private key used for signing assertion by BIG-IP as IdP.
- **location-specific**
  Objects of this class might have location specific attribute(s). Admin can indicate if object is location specific by setting it to true.
- **log-level**
  Specifies log level for this SAML SSO object.

- **metadata-cert**
  Specifies the certificate with public key of the key pair used in signing the metadata. See export-metadata for more information on metadata export functionality. This is the certificate to includ in signed metadata when we export metadata. This might or might not be IdP certificate.
- **metadata-file**
  Specifies the file to which metadata is saved. See export-metadata for more information on metadata export functionality.
- **metadata-signkey**
  This specifies the key that is used to sign IdP's metadata. See export-metadata for more information on metadata export functionality.
- **sp-connectors**
  Specifies list of SP connectors associated with this SAML SSO object. When this SSO object is assigned to SAML resource then only one entry is allowed for SP connectors. If SAML SSO object is assigned to access profile then you can add multiple SAML SP connectors.
- **subject-type**
  Specifies type of the subject to be used while creating SAML assertion.
- **subject-value**
  Specifies the value of the subject to be included inside SAML assertion. This can be a session variable. For example: %{session.last.logonname}, %{session.ad.last.attr.userEmail}

saml-resource

Configures saml resource.

Syntax

Configure a **saml-resource** using the syntax shown in the following sections.

Create/Modify

```
create saml-resource [name]
modify saml-resource [name]
    app-service [[string] | none]
    customization-group [[string] | none]
    description [[string] | none]
    location-specific [true | false]
    publish-on-webtop [true | false]
    sso-config-saml [[string] | none]
edit saml-resource [ [ [name] | [glob] | [regex] ] ... ]
    all-properties
    non-default-properties
```

Display

```
list saml-resource
list saml-resource [ [ [name] | [glob] | [regex] ] ... ]
show running-config saml-resource
show running-config saml-resource [ [ [name] | [glob] | [regex] ] ... ]
    all-properties
    non-default-properties
    one-line
```

Delete

```
delete saml-resource [name]
```

Description

You can use **saml-resource** component to configure saml resource.

Examples

- **create saml-resource my_saml_resource { sso-config-saml my_saml_sso_obj publish-on-webtop true }**
  Creates a saml resource named **my_saml_resource** with saml sso object ‘my_saml_sso_obj’ and with option to display this resource on full webtop.

- **delete saml-resource my_saml_resource**
  Deletes the saml resource named **my_saml_resource**.

Options

- **app-service**
  Specifies the name of the application service to which the object belongs. The default value is **none**. **Note:** If the **strict-updates** option is **enabled** on the application service that owns the object, you cannot modify or delete the object. Only the application service can modify or delete the object.
- **customization-group**
  Specifies the customization group associated with saml resource.
- **description**
  Specifies a description for the saml resource. The default is **none**.
- **location-specific**
  Specifies whether or not this object contains one or more attributes with values that are specific to the location where the BIG-IP device resides. The location-specific attribute is either true or false. When using policy sync, mark an object as location-specific to prevent errors that can occur when policies reference objects, such as authentication servers, that are specific to a certain location.
- **publish-on-webtop**
  Specifies whether saml resource to be displayed on full webtop or not. Default value is ‘true’.
- **sso-config-saml**
  Specifies saml sso config object associated with this saml resource. This saml sso object should only have one saml sp connector associated with it.

saml-sp-connector

Specify saml sp connector configuration.

Syntax

Configure a **saml-sp-connector** within the **sso** module using the syntax shown in the following sections.

Create/Modify

```
create saml-sp-connector [name]
modify saml-sp-connector [name]
    app-service [[string] | none]
    assertion-consumer-binding [http-artifact | http-post]
    assertion-consumer-uri [string]
    description [[string] | none]
    encryption-type [aes128 | aes192 | aes256]
    entity-id [string]
    import-metadata [ string | none ]
    is-authn-request-signed [ true | false ]
    location-specific [ true | false ]
    metadata-cert [[string] | none]
    relay-state [[string] | none]
    sign-artifact-resolution-rq [true | false]
    sp-certificate [[string] | none]
    want-assertion-encrypted [ true | false ]
    want-assertion-signed [ true | false ]
    want-response-signed [ true | false ]
edit saml-sp-connector [ [ [name] | [glob] | [regex] ] ... ]
    all-properties
    non-default-properties
```

Display

```
list saml-sp-connector
list saml-sp-connector [ [ [name] | [glob] | [regex] ] ... ]
show running-config saml-sp-connector
show running-config saml-sp-connector [ [ [name] | [glob] | [regex] ] ... ]
    all-properties
    app-service
    non-default-properties
    one-line
    partition
```

Delete

```
delete saml-sp-connector [name]
```

Description

You can use the **saml-sp-connector** component to create and manage saml sp connectors

Examples

- **create saml-sp-connector my_saml_sp_connector { entity-id "https://companyx.sp.com/sp" assertion-consumer-uri "https://companyx.sp.com/acs/" want-assertion-signed true want-response-signed true want-assertion-encrypted true encryption-type aes256 is-authn-request-signed false sp-certificate default.crt }**
  Creates a SAML sp-connector named **my_saml_sp_connector** with security options to encrypt and sign the assertion as well as SAML response.
- **create saml-sp-connector my_saml_sp_connector1 { import-metadata /shared/tmp/sp_metadata.xml}**
  Creates a SAML sp-connector named **my_saml_sp_connector1** from metadata file "/shared/tmp/sp_metadata.xml"
- **list saml-sp-connector**
  Displays a list of SAML sp connectors.
- **delete saml-sp-connector my_saml_sp_connector**
  Deletes the **my_saml_sp_connector** SAML sp connector.

Options

- **app-service**
  Specifies the name of the application service to which the object belongs. The default value is **none**. **Note:** If the **strict-updates** option is **enabled** on the application service that owns the object, you cannot modify or delete the object. Only the application service can modify or delete the object.
- **assertion-consumer-binding**
  Specifies the method that the SP uses to receive assertions from BIG-IP as IdP. Default value is **http-post**.
- **assertion-consumer-uri**
  Specifies the URL of SP's ACS service where BIG-IP as IdP sends assertion.
- **description**
  Specifies a unique description for saml sp connector. The default is **none**.
- **encryption-type**
  Specifies the type of encryption BIG-IP as IdP should use to encrypt the assertion. Default is aes128.
- **entity-id**
  Specifies unique URI to identify SP pointed by sp connector.
- **import-metadata**
  Specifies the metadata file to be used to create sp connector object. For example: **create saml-sp-connector my_saml_sp_connector1 { import-metadata /shared/tmp/sp_metadata.xml}**

- **is-authn-request-signed**
  Specifies whether SP signs authentication requests while sending them to BIG-IP as IdP. The default value for this is **false**.
- **location-specific**
  Objects of this class might have location specific attribute(s). Admin can indicate if object is location specific by setting it to true.
- **metadata-cert**
  Specifies the certificate to be used to verify the signature of metadata imported from a file.
- **relay-state**
  Specifies the value sent to the SP by BIG-IP as IdP as part of the response. This value is only used if the SP did not send RelayState as part of the authentication request.
- **sign-artifact-resolution-rq**
  Specifies whether this BIG-IP as IdP requires artifact resolve requests to be signed. The default value is true.
- **sp-certificate**
  Specifies SP certificate used by BIG-IP as IdP to verify the signature of authentication request.
- **want-assertion-encrypted**
  Specifies whether SP requires encrypted assertions. The default value for this attribute is **false**
- **want-assertion-signed**
  Specifies whether SP requires signed assertions. The default value for this attribute is **true**
- **want-response-signed**
  Specifies whether SP requires signed SAML responses. The default value for this attribute is **false**

41

asm

- Introducing the asm module
- Alphabetical list of components

Introducing the asm module

You can use the tmsh components that reside within the asm module to configure BIG-IP® Application Security Manager™. For more information about the tmsh hierarchical structure, see Chapter 2, *Understanding and Using the Traffic Management Shell*.

Alphabetical list of components

The remainder of this chapter lists the tmsh components that are available in the asm module.

device-sync

Contains the ASM timestamp for each device in the group.

Syntax

Retrieve the list of the **device-sync** values using the syntax shown in the following section.

Display

```
list device-sync
list device-sync [ [ [name] | [glob] | [regex] ] ... ]
```

Description

Use this command to display the current values of the device-sync object, i.e. ASM change times for all devices in the group. This object is designed for internal purposes only (incremented on every ASM change), so do not try to create, modify, or delete it manually.

Examples

list device-sync

Displays all last ASM change times of the device group.

See Also

tmsh, *list*, glob, regex

http-method

Lists the available HTTP request methods that can be used in the context of the Application Security Manager™.

Syntax

Retrieve the list of the **http-method** values using the syntax shown in the following sections.

Display

```
list http-method
list http-method [ [ [name] | [glob] | [regex] ] ... ]
    all
    app-service
    default-act-as
    one-line
    partition
    recursive
```

Description

Use this command to display the possible values of the http-method object to be used in the context of the Application Security Manager. These possible values include predefined and user-defined allowed methods for all security policies, and also are intended to be used in filters of Application Security Logging and in HTTP security profiles.

Examples

list http-method

Displays all the HTTP methods supported by the ASM.

Options

- **app-service**
  Displays the application service to which the object belongs. The default value is **none**. **Note:** If the **strict-updates** option is **enabled** on the Application Service that owns the object, you cannot modify or delete the object. Only the Application Service can modify or delete the object.
- **default-act-as**
  Displays the HTTP request method, either GET or POST, based on how you have instructed the system to treat the listed method name; a predefined method has its system default and a user-defined allowed method is configured in the security policy.

- **partition**
  Displays the administrative partition within which the component resides.

See Also

glob, *list*, regex, *profile*, *profile*, *tmsh*

httpclass-asm

configure initial ASM settings for applications. This component has been deprecated as of BIG-IP v11.3.0, please use the **policy** component in the **asm** module instead.

Syntax

Configure the **httpclass-asm** component within the **asm** module using the syntax shown in the following sections.

Create/Modify

```
create httpclass-asm [name]
modify httpclass-asm [name]
    active-policy-name [string]
    app-service [[string] | none]
    language [language]
    predefined-policy [predefined-policy]
```

Display

```
list httpclass-asm
list httpclass-asm [ [ [name] | [glob] | [regex] ] ... ]
show running-config httpclass-asm
show running-config httpclass-asm [ [ [name] | [glob] | [regex] ] ... ]
    all-properties
    non-default-properties
    partition
```

Delete

```
delete httpclass-asm [name]
```

Description

Use this command to create, modify, display, or delete an httpclass-asm profile that configures ASM security policies. Changing/setting attributes for an httpclass-asm profile affects the ASM security policy with the same name. Note that modifying the language of an existing profile reconfigures the ASM security policy and deletes the configurations, log entries and statistics of the security policy. This is for advanced usage - this command is intended to be used by the application templates system (iApps™).

Examples

create asm httpclass-asm my_class active-policy-name my_class_policy language utf-8 predefined-policy POLICY_TEMPLATE_RAPID_DEPLOYMENT_HTTP

Creates a custom httpclass-asm profile named **my_class** that causes ASM to configure a security policy that uses the utf-8 application language and the Rapid Deployment security policy.

list httpclass-asm

Displays the properties of all httpclass-asm profiles.

Options

- **active-policy-name**
  Specifies the name of the active security policy. This property has been deprecated. As of BIG-IP v11.1.0, the active security policy name is identical to the HTTP class profile's name.
- **app-service**
  Specifies the name of the application service to which the object belongs. The default value is **none**. **Note:** If the **strict-updates** option is **enabled** on the application service that owns the object, you cannot modify or delete the object. Only the application service can modify or delete the object.
- **language**
  Specifies the language of the web application that the ASM security policy is protecting. Use autocomplete or **list /asm webapp-language** to get the list of supported languages.
- **name**
  Specifies a unique name for the component. This option is required for the commands **create**, **delete**, and **modify**.
- **predefined-policy**
  Specifies a predefined security policy for a web application. This security policy was prebuilt to provide out of the box security for a known application. Use autocomplete to get a list of applications for which ASM has predefined policies.

See Also

create, *delete*, *edit*, glob, *list*, *virtual*, *modify*, regex, *reset-stats*, *show*, *tmsh*

policy

Configures an application security policy.

Syntax

Configure the **policy** component within the **asm** module using the syntax shown in the following sections.

Create/Modify

```
create policy [name]
modify policy [name]
    [active | inactive]
    app-service [[string] | none]
    blocking-mode [enabled | disabled]
    description [[string] | none]
    encoding [[name] | none]
    policy-builder [enabled | disabled]
    policy-template [name]
```

Display

```
list policy [ [ [name] | [glob] | [regex] ] ... ]
show running-config policy [ [ [name] | [glob] | [regex] ] ... ]
    all-properties
    one-line
    partition
    virtual-servers
```

Delete

```
delete policy [name]
```

Save

```
save policy [name]
    overwrite
    bin-file [filename]
    min-xml-file [filename]
    xml-file [filename]
```

Load

```
load policy [name]
    overwrite
    file [filename]
    xml-string [string]
```

Publish

```
publish policy [name]
```

Description

You can use the **policy** component to create, modify, display, delete, save, load, or publish an application security policy for use with Application Security Manager functionality.

◆ Note

*To display all policy properties available in **tmsh**, including initial settings used by iApp and advanced configuration accessible in ASM GUI, specify the **all-properties** option or the detailed properties. By default, only initial properties are displayed: **encoding**, **policy-template** and **[active | inactive]**.*

◆ Note

*The **modify** command with the properties **encoding** and/or **policy-template** causes ASM to reconfigure the security policy and clear all its former data.*

Examples

create policy my_asm_policy encoding utf-8

Creates a new policy named **my_asm_policy** with the default language encoding.

modify policy my_asm_policy active

Activates the inactive policy named **my_asm_policy**.

list policy

Displays the properties of all application security policies.

save policy my_asm_policy xml-file my_asm_policy.xml

Exports the policy named **my_asm_policy** to the XML file **/var/tmp/my_asm_policy.xml**.

load policy my_asm_policy overwrite file /tmp/my_asm_policy.plc

Imports the policy named **my_asm_policy** from the file **/tmp/my_asm_policy.plc** and overwrites the policy if it already exists.

publish policy my_asm_policy

Applies the active policy named **my_asm_policy**.

Options

- **app-service**
  Specifies the name of the application service to which the object belongs. The default value is **none**. **Note:** If the **strict-updates** option is **enabled** on the application service that owns the object, you cannot modify or delete the object. Only the application service can modify or delete the object.

- **[active | inactive]**
  Activates or deactivates the policy for later association with L7 policies and virtual servers. The default value is **inactive**.
- **bin-file**
  Specifies the exported file name to be saved in binary format when using the **save** command. The file name should be simple (not a full path); it is saved to the **/var/tmp** directory on the system.
- **blocking-mode**
  Specifies whether the system blocks a request that triggers a security policy violation or only logs the violation event (transparent mode).
- **description**
  Specifies an optional description of the security policy.
- **encoding**
  Specifies the language encoding, which determines how the security policy processes the character sets. This property corresponds to the **language** property of the **httpclass-asm** component.
- **file**
  Specifies the file name from which the policy is going to be imported when using the **load** command. A full path should be specified.
- **glob**
  Displays the items that match the **glob** expression. See **help glob** for a description of **glob** expression syntax.
- **min-xml-file**
  Specifies the exported file name to be saved in compact XML format when using the **save** command. The file name should be simple (not a full path); it is saved to the **/var/tmp** directory on the system. To display the XML output immediately, omit this property, the properties **xml-file** and **bin-file**.
- **name**
  Specifies a unique name for the component. This option is required for the commands **create**, **delete**, **modify**, **save**, and **publish**. If it is not specified for the **load** command, the policy name will be taken from the imported settings.
- **overwrite**
  Specifies that the policy file for the **save** command or the policy component for the **load** command can be overwritten if it exists.
- **partition**
  Displays the administrative partition within which the component resides.
- **policy-builder**
  Enables or disables automatic policy building.
- **policy-template**
  Specifies whether the security policy is based on a predefined security policy template, and if so, which one. If you create or modify a security policy based on a template, the system automatically configures the new

security policy according to the conditions of the template. This property corresponds to the **predefined-policy** property of the **httpclass-asm** component.

- **regex**
  Displays the items that match the regular expression. The regular expression must be preceded by an at sign (@[regular expression]) to indicate that the identifier is a regular expression. See **help regex** for a description of regular expression syntax.

◆ Note

*This component supports matching by the **regex** expression only when displaying the initial policy properties.*

- **virtual-servers**
  Displays the name of the protected virtual server, or virtual servers, which have attached to them the security policy via L7 policies.
- **xml-file**
  Specifies the exported file name to be saved in XML format when using the **save** command. The file name should be simple (not a full path); it is saved to the **/var/tmp** directory on the system. To display the XML output immediately, omit this property, the properties **min-xml-file** and **bin-file**.
- **xml-string**
  Specifies the XML document from which the policy is going to be imported when using the **load** command.

See Also

predefined-policy, *webapp-language*, *create*, *delete*, glob, *list*, *load*, *policy*, *virtual*, *modify*, *publish*, regex, *save*, *tmsh*

predefined-policy

Lists the available predefined policies that can be used in the context of the **httpclass-asm** profile.

Syntax

Retrieve the list of the **predefined-policy** values using the syntax shown in the following sections.

Display

```
list predefined-policy
list predefined-policy [ [ [name] | [glob] | [regex] ] ... ]
    all
    one-line
```

Description

Use this command to display the possible values of the predefined-policy object to be used in the context of the httpclass-asm profile. This is for advanced usage; this command is intended for use by the application templates system (iApps).

Examples

list predefined-policy

Displays all the predefined policies supported by the ASM.

See Also

httpclass-asm, glob, *list*, regex, *tmsh*

response-code

Lists the available HTTP response status codes that can be used in the context of the Application Security Manager.

Syntax

Retrieve the list of the **response-code** values using the syntax shown in the following sections.

Display

```
list response-code
list response-code [ [ [number] | [glob] | [regex] ] ... ]
    all
    app-service
    name
    one-line
```

Description

Use this command to display the possible values of the response-code object to be used in the context of the Application Security Manager. These possible values are predefined and intended to be used in filters of Application Security Logging.

Examples

list response-code

Displays all the response codes supported by the ASM.

Options

- **app-service**
  Displays the application service to which the object belongs. The default value is **none**. **Note:** If the **strict-updates** option is **enabled** on the Application Service that owns the object, you cannot modify or delete the object. Only the Application Service can modify or delete the object.
- **name**
  Displays a well-known textual meaning of the HTTP response code.

See Also

glob, *list*, regex, *profile*, *tmsh*

webapp-language

Lists the available languages that can be used in the context of the httpclass-asm profile.

Syntax

Retrieve the list of the **webapp-language** values using the syntax shown in the following sections.

Display

```
list webapp-language
list webapp-language [ [ [name] | [glob] ... ]
    all
    one-line
```

Description

Use this command to display the possible values of the webapp-language object to be used in the context of the httpclass-asm profile. This is for advanced usage - this command is intended to be used by the application templates system.

Examples

list webapp-language

Displays all the languages supported by the ASM.

See Also

httpclass-asm, glob, *list*, *tmsh*

42

auth

- Introducing the auth module
- Alphabetical list of components

Introducing the auth module

You can use the tmsh components that reside within the auth module to configure user authentication. For more information about the tmsh hierarchical structure, see Chapter 2, *Understanding and Using the Traffic Management Shell*.

Alphabetical list of components

The remainder of this chapter lists the tmsh components that are available in the auth module.

apm-auth

Configures an APM-based authentication object for implementing access policy execution-based authentication of BIG-IP® system users.

Syntax

Configure the **apm-auth** component within the **auth** module using the syntax shown in the following sections.

Create/Modify

```
create apm-auth [name]
modify apm-auth [name]
    profile-access [string]
edit apm-auth [ [ [name] | [glob] | [regex] ] ...]
    all-properties
    non-default-properties
```

Display

```
list apm-auth
list apm-auth [ [ [name] | [glob] | [regex] ] ...]
show running-config apm-auth
show running-config apm-auth [ [ [name] | [glob] | [regex] ] ...]
    all-properties
    non-default-properties
    one-line
    partition
```

Delete

```
delete apm-auth [name]
```

Description

You can configure APM-based authentication to execute an access policy for BIG-IP system users to authenticate and authorize them.

APM authentication methods like HTTP, AD/LDAP, TACACS+ authentication can be used in box authentication To authenticate BIG-IP system users.To do this, create an access profile, create APM configuration object with the above access profile, and then activate the object.

The following steps describe how to configure APM-based authentication for BIG-IP system users:

1. Use the **profile-access** component in the **apm** module to create a access profile.

2. Use the **apm-auth** component in the **auth** module to map an access profile to an APM-based authentication object.

3. To activate APM-based authentication for BIG-IP system users, run the command sequence **modify / auth source type apm-auth**

Examples

create apm-auth system-auth {profile-access apm-profile}

Creates an APM-based authentication object named **system-auth**

delete apm-auth system-auth

Deletes the APM-based authentication object named **system-auth**.

Options

- **description**
  User-defined description.
- **glob**
  Displays the items that match the glob expression. See help glob for a description of glob expression syntax.
- **name**
  Specifies a unique name for the component. This option is required for the commands **create** and **modify**.
- **partition**
  Displays the administrative partition within which the component resides.
- **profile-access**
  Specifies the access profile that the system must use for APM-based authentication. You must specify an access profile when you create an APM-based configuration object.
- **regex**
  Displays the items that match the regular expression. The regular expression must be preceded by an at sign (@[regular expression]) to indicate that the identifier is a regular expression. See **help regex** for a description of regular expression syntax.

See Also

user, *create*, *delete*, glob, *list*, *modify*, regex, *run*, *show*, *tmsh*

cert-ldap

Configures an LDAP configuration object for implementing Single Sign On based on a valid client certificate for BIG-IP® system users. The user is required to properly configure the apache for client certificate validation.

Syntax

Configure the **cert-ldap** component within the **auth** module using the syntax shown in the following sections.

Create/Modify

```
create cert-ldap [name]
modify cert-ldap [name]
    bind-dn [ [account dn] | none]
    bind-pw [none | [password] ]
    bind-timeout [integer]
    check-host-attr [disabled | enabled]
    check-roles-group [disabled | enabled]
    debug [disabled | enabled]
    description [string]
    filter [ [filter name] | none]
    idle-timeout [integer]
    ignore-auth-info-unavail [no | yes]
    ignore-unknown-user [disabled | enabled]
    login-attribute [ [account name] | none]
    login-filter [ [string] | none]
    login-name [ [ldap attribute] | none]
    port [ [name] | [integer]]
    scope [base | one | sub]
    search-base-dn [[search base dn] | none]
    search-timeout [integer]
    servers [add | delete | replace-all-with] {
      [ [ip address] | [server name] ...] }
    servers none
    ssl [disabled | enabled]
    ssl-ca-cert-file [ [file name] | none)
    ssl-check-peer [disabled | enabled]
    ssl-ciphers [ [string] | none]
    ssl-client-cert [ [string] | none]
    ssl-client-key [ [string] | none]
    sso [on | off]
    version [integer]
    warnings [disabled | enabled]
edit cert-ldap [ [ [name] | [glob] | [regex] ] ...]
    all-properties
    non-default-properties
```

Display

```
list cert-ldap
list cert-ldap [ [ [name] | [glob] | [regex] ] ...]
show running-config cert-ldap
show running-config cert-ldap [ [ [name] | [glob] | [regex] ] ...]
    all-properties
```

```
non-default-properties
one-line
partition
```

Delete

```
delete cert-ldap [name]
```

Description

The CERT-LDAP authentication mode is required to provide Single Sign On capability to the control plane based on a valid client certificate. This mode involves configuring an Apache server to initiate a client certificate request, perform certificate validation against an OCSP server, and then authenticate/authorize certificate credentials against a configured remote LDAP server or a Microsoft® Windows® Active Directory®. The mode is not based on basic HTTP authentication (that is, user name and password). CERT-LDAP mode is equivalent to LDAP mode with custom attributes.

To authenticate BIG-IP system users when their authentication data is stored on a remote LDAP server, you create an LDAP configuration object, and then activate the object. Make sure that Apache is configured to support the client certificate validation.

To configure CERT-LDAP authentication for BIG-IP system users:

1. Use the **cert-ldap** component in the **auth** module to configure an LDAP configuration object.

2. To activate LDAP authentication for BIG-IP system users, run the command sequence **modify / auth source type cert-ldap**

Examples

create cert-ldap bigip_cert_ldap_auth servers add {my_ldap_server}

Creates a configuration object named **bigip_cert_ldap_auth**.

delete cert-ldap bigip_cert_ldap_auth

Deletes the configuration object named **bigip_cert_ldap_auth**.

Options

- **bind-dn**
  Specifies the distinguished name of an account to which to bind to perform searches. This search account is a Read-only account. You can

also use the **admin** account as the search account. If an administrative distinguished name is not specified, then a bind is not attempted. The default value is **none**.

◆ Note

If the remote server is a Microsoft Windows Active Directory server, the distinguished name must be in the form of an email address.

- **bind-pw**
  Specifies the password for the search account created on the LDAP server. This option is required if you enter a value for the **bind-dn** option. The default value is **none**.
- **bind-timeout**
  Specifies a bind timeout limit, in seconds. The default value is **30**.
- **check-host-attr**
  Confirms the password for the bind distinguished name. This option is optional. The default value is **disabled**.
- **check-roles-group**
  Specifies whether to verify a user's group membership given in the remote-role definitions, formatted as ***member*of=''group-dn''**. The default value is **disabled**.
- **debug**
  Enables or disables **syslog-ng** debugging information at the LOG DEBUG level. The default value is **disabled**. F5 Networks does not recommend using this option for normal configuration.
- **description**
  User defined description.
- **filter**
  Specifies a filter. Use this option for authorizing client traffic. The default value is **none**.
- **glob**
  Displays the items that match the **glob** expression. See **help glob** for a description of **glob** expression syntax.
- **group-dn**
  Specifies the group distinguished name. The system uses this option for authorizing client traffic. The default value is **none**.
- **group-member-attribute**
  Specifies a group member attribute. The system uses this option for authorizing client traffic. The default value is **none**.
- **idle-timeout**
  Specifies the idle timeout, in seconds, for connections. The default value is **3600** seconds.
- **ignore-auth-info-unavail**
  Specifies whether the system ignores authentication information if it is not available. The default value is **no**.

- **ignore-unknown-user**
  Specifies whether the system ignores a user that is unknown. The default value is **disabled**.
- **login-attribute**
  Specifies a logon attribute. Normally, the value for this option is **uid**; however, if the server is a Microsoft Windows Active Directory server, the value must be the account name **samaccountname** (not case-insensitive). The default value is **none**.
- **login-filter**
  Specifies the filter to be applied on the CN of the client certificate. This filter is a regular expression to extract required information from CN of client certificate which will be used to match against LDAP search results. The default is **disabled**.
- **login-name**
  Specifies the ldap attribute to be used as a login name. The default is **disabled**.
- **name**
  Specifies a unique name for the component. This option is required for the commands **create** and **modify**.
- **partition**
  Displays the administrative partition within which the component resides.
- **port**
  Specifies the port number or name for the LDAP service. Port **389** is typically used for non-SSL and port **636** is used for an SSL-enabled LDAP service. The default value is **ldap**.
- **regex**
  Displays the items that match the regular expression. The regular expression must be preceded by an at sign (@[regular expression]) to indicate that the identifier is a regular expression. See **help regex** for a description of regular expression syntax.
- **scope**
  Specifies the search scope. The default value is **sub**. The possible values are:
  - **base**
    The search scope is base object. The **base** value is almost never useful for name service lookups.
  - **one**
    The search scope is one level.
  - **sub**
    The search scope is a subtree.
- **search-base-dn**
  Specifies the search base distinguished name. The default value is **none**.
- **search-timeout**
  Specifies the search timeout, in seconds. The default value is **30**.

- **servers**
  Specifies the LDAP servers that the system must use to obtain authentication information. You must specify a server when you create an LDAP configuration object.
- **ssl**
  Enables or disables SSL functionality. The default is **disabled**.
  Note that when you use **tmsh** to enable SSL for an LDAP service, the system does not change the port number from **389** to **636**, as is required. To change the port number from the command line, use the **port** option, for example, **ldap [name] ssl enabled port 636**.
- **ssl-ca-cert-file**
  Specifies the name of an SSL CA certificate using the full path to the file. The default value is **none**.
- **ssl-check-peer**
  Specifies whether the system checks an SSL peer. The default value is **disabled**.
- **ssl-ciphers**
  Specifies SSL ciphers. The default value is **none**.
- **ssl-client-cert**
  Specifies the name of an SSL client certificate. The default value is **none**.
- **ssl-client-key**
  Specifies the name of an SSL client key. The default value is **none**.
- **sso**
  Enables or disables Single Sign On (SSO) functionality. SSO eliminates the need to administer and maintain multiple user logons and eliminates the need for users to enter their credentials multiple times. When SSO is disabled, the user will be prompted to authenticate into the BIG-IP. The default is **off**.
- **user-template**
  Specifies a user template for the LDAP application to use for authentication. The default value is **none**.
- **version**
  Specifies the version number of the LDAP application. The default value is **3**.
- **warnings**
  Enables or disables warning messages. The default value is **enabled**.

See Also

user, *create*, *delete*, glob, *list*, *modify*, regex, *run*, *show*, *tmsh*

ldap

Configures an LDAP configuration object for implementing remote LDAP-based authentication of BIG-IP® system users.

Syntax

Configure the **ldap** component within the **auth** module using the syntax shown in the following sections.

Create/Modify

```
create ldap [name]
modify ldap [name]
    bind-dn [ [account dn] | none]
    bind-pw [none | [password] ]
    bind-timeout [integer]
    check-host-attr [disabled | enabled]
    check-roles-group [disabled | enabled]
    debug [disabled | enabled]
    description [string]
    filter [ [filter name] | none]
    group-dn [ [group dn] | none]
    group-member-attr [ [attribute] | none]
    idle-timeout [integer]
    ignore-auth-info-unavail [no | yes]
    ignore-unknown-user [disabled | enabled]
    login-attribute [ [account name] | none]
    port [ [name] | [integer]]
    scope [base | one | sub]
    search-base-dn [[search base dn] | none]
    search-timeout [integer]
    servers [add | delete | replace-all-with] {
        [ [ip address] | [server name] ...] }
    servers none
    ssl [disabled | enabled]
    ssl-ca-cert-file [ [file name] | none)
    ssl-check-peer [disabled | enabled]
    ssl-ciphers [ [string] | none]
    ssl-client-cert [ [string] | none]
    ssl-client-key [ [string] | none]
    user-template [ [string] | none]
    version [integer]
    warnings [disabled | enabled]
edit ldap [ [ [name] | [glob] | [regex] ] ...]
    all-properties
    non-default-properties
```

Display

```
list ldap
list ldap [ [ [name] | [glob] | [regex] ] ...]
show running-config ldap
show running-config ldap [ [ [name] | [glob] | [regex] ] ...]
    all-properties
```

```
non-default-properties
one-line
partition
```

Delete

```
delete ldap [name]
```

Description

LDAP authentication is useful when the BIG-IP system users authentication or authorization data is stored on a remote LDAP server or a Microsoft® Windows® Active Directory® server, and you want the user credentials to be based on basic HTTP authentication (that is, user name and password).

To authenticate BIG-IP system users when their authentication data is stored on a remote LDAP server, you create an LDAP configuration object, and then activate the object.

The following steps describe how to configure LDAP authentication for BIG-IP system users:

1. Use the **ldap** component in the **auth** module to configure an LDAP configuration object.

2. To activate LDAP authentication for BIG-IP system users, run the command sequence **modify / auth source type ldap**

Examples

create ldap bigip_ldap_auth servers add {my_ldap_server}

Creates a configuration object named **bigip_ldap_auth**

delete ldap bigip_ldap_auth

Deletes the configuration object named **bigip_ldap_auth**.

Options

- **bind-dn**
  Specifies the distinguished name of an account to which to bind to perform searches. This search account is a Read-only account. You can also use the **admin** account as the search account. If an administrative distinguished name is not specified, then a bind is not attempted. The default value is **none**.
  Note that if the remote server is a Microsoft Windows Active Directory server, the distinguished name must be in the form of an email address.
- **bind-pw**
  Specifies the password for the search account created on the LDAP server. This option is required if you enter a value for the **bind-dn** option. The default value is **none**.

- **bind-timeout**
  Specifies a bind timeout limit, in seconds. The default value is **30**.
- **check-host-attr**
  Confirms the password for the bind distinguished name. This option is optional. The default value is **disabled**.
- **check-roles-group**
  Specifies whether to verify a user's group membership given in the remote-role definitions, formatted as ***member*of="group-dn"**. The default value is **disabled**.
- **debug**
  Enables or disables **syslog-ng** debugging information at the LOG DEBUG level. The default value is **disabled**. F5 Networks does not recommend using this option for normal configuration.
- **description**
  User defined description.
- **filter**
  Specifies a filter. Use this option for authorizing client traffic. The default value is **none**.
- **glob**
  Displays the items that match the **glob** expression. See **help glob** for a description of **glob** expression syntax.
- **group-dn**
  Specifies the group distinguished name. The system uses this option for authorizing client traffic. The default value is **none**.
- **group-member-attribute**
  Specifies a group member attribute. The system uses this option for authorizing client traffic. The default value is **none**.
- **idle-timeout**
  Specifies the idle timeout, in seconds, for connections. The default value is **3600** seconds.
- **ignore-auth-info-unavail**
  Specifies whether the system ignores authentication information if it is not available. The default value is **no**.
- **ignore-unknown-user**
  Specifies whether the system ignores a user that is unknown. The default value is **disabled**.
- **login-attribute**
  Specifies a logon attribute. Normally, the value for this option is **uid**; however, if the server is a Microsoft Windows Active Directory server, the value must be the account name **samaccountname** (not case-insensitive). The default value is **none**.
- **name**
  Specifies a unique name for the component. This option is required for the commands **create** and **modify**.
- **partition**
  Displays the administrative partition within which the component resides.

- **port**
  Specifies the port number or name for the LDAP service. Port **389** is typically used for non-SSL and port **636** is used for an SSL-enabled LDAP service. The default value is **ldap**.
- **regex**
  Displays the items that match the regular expression. The regular expression must be preceded by an at sign (@[regular expression]) to indicate that the identifier is a regular expression. See **help regex** for a description of regular expression syntax.
- **scope**
  Specifies the search scope. The default value is **sub**. The possible values are:
  - **base**
    The search scope is base object. The **base** value is almost never useful for name service lookups.
  - **one**
    The search scope is one level.
  - **sub**
    The search scope is a subtree.
- **search-base-dn**
  Specifies the search base distinguished name. The default value is **none**.
- **search-timeout**
  Specifies the search timeout, in seconds. The default value is **30**.
- **servers**
  Specifies the LDAP servers that the system must use to obtain authentication information. You must specify a server when you create an LDAP configuration object.
- **ssl**
  Enables or disables SSL functionality. The default is **disabled**.
  Note that when you use **tmsh** to enable SSL for an LDAP service, the system does not change the port number from **389** to **636**, as is required. To change the port number from the command line, use the **port** option, for example, **ldap [name] ssl enabled port 636**.
- **ssl-ca-cert-file**
  Specifies the name of an SSL CA certificate using the full path to the file. The default value is **none**.
- **ssl-check-peer**
  Specifies whether the system checks an SSL peer. The default value is **disabled**.
- **ssl-ciphers**
  Specifies SSL ciphers. The default value is **none**.
- **ssl-client-cert**
  Specifies the name of an SSL client certificate. The default value is **none**.
- **ssl-client-key**
  Specifies the name of an SSL client key. The default value is **none**.

- **user-template**
  Specifies a user template for the LDAP application to use for authentication. The default value is **none**.
- **version**
  Specifies the version number of the LDAP application. The default value is **3**.
- **warnings**
  Enables or disables warning messages. The default value is **enabled**.

See Also

user, *create*, *delete*, glob, *list*, *modify*, regex, *run*, *show*, *tmsh*

login-failures

Displays or resets the status of the accounts of users whose attempts to log in to the BIG-IP® system have failed.

Syntax

Configure the **login-failures** component within the **auth** module using the following syntax.

Modify

```
reset-stats login-failures
    username
```

Display

```
show login-failures
    field-fmt
    username
```

Description

Users assigned a role of **Administrator** can reset the status of a user who is locked out of the BIG-IP system due to enforcement of a company's security requirements. Users assigned other roles can only view login failures.

Examples

show login-failures

Displays the login failure status of all users.

show login-failures joe

Displays login failure status for the user joe.

reset-stats login-failures

Resets the failed login counters for all users to zero and unlocks all users.

reset-stats login-failures joe

Resets the failed login counter for the user joe to zero and unlocks the user joe.

Options

- **show**
  For information about the options that you can use with the **show** command, see **help show**.
- **username**
  Specifies a user account to display or reset.

See Also

user, *reset-stats*, *show*, *tmsh*

partition

Configures administrative partitions that implement access control for BIG-IP® system users.

Syntax

Configure the **partition** component within the **auth** module using the syntax shown in the following sections.

Create/Modify

```
create partition [name]
modify partition [name]
    default-route-domain [ID]
    description [string]
```

Display

```
list partition
list partition [ [ [name] | [glob] | [regex] ] ...]
show running-config partition
show running-config partition [ [ [name] | [glob] | [regex] ] ...]
    all-properties
    non-default-properties
    one-line
```

Delete

```
delete partition [name]
    all
```

Description

An administrative partition is a logical container that you create, containing a defined set of BIG-IP system objects, such as virtual servers, pools, and profiles. When a specific set of objects resides in a partition, you can then give certain users the authority to view and manage the objects in that partition only, rather than all objects on the BIG-IP system. This gives a finer degree of administrative control.

You can configure administrative partitions, only if the **Administrator** user role is assigned to your user account.

Examples

create partition partition_A description "Repository for application_A objects"

Creates a partition named **partition_A** that contains objects related to application_A.

delete partition partition_B

Deletes the partition named **partition_B**.

Options

- **description**
  Describes the contents of the partition. If you use spaces in the description, you must put quotation marks around the descriptive text, for example, "This partition contains local traffic management objects for managing HTTP traffic."
- **default-route-domain**
  Specifies the ID of the route domain that is associated with the IP addresses that reside in the partition. For more information, see **help net route-domain**.
- **glob**
  Displays the items that match the **glob** expression. See **help glob** for a description of **glob** expression syntax.
- **name**
  Specifies a unique name for the component. This option is required for the commands **create** and **modify**.
- **regex**
  Displays the items that match the regular expression. The regular expression must be preceded by an at sign (@[regular expression]) to indicate that the identifier is a regular expression. See **help regex** for a description of regular expression syntax.

See Also

user, *create*, *delete*, glob, *list*, *modify*, *route-domain*, regex, *show*, *tmsh*

password

Prompts for modification of a password, and asks for a confirmation of the new password.

Syntax

Configure the **password** component within the **auth** module using the syntax shown in the following sections.

Usage

```
modify password
```

Description

If you are assigned the user role of **Administrator** or **User Manager**, you can change another user's password.

For example, from within the **auth** module, run the following command sequence: **modify password [user name]**.

The system prompts you for a new password for the specified user, and then to confirm the new password.

If you are assigned any other user role, the system prompts you to change your own password, and then confirm the new password.

To change a password from within another module, use the full path to the password.

Examples

(tmos.auth)# modify password

From within the **auth** module, displays the **new password:** prompt.

(tmos.gtm)# modify / auth password

From within the **gtm** module, displays the **new password:** prompt.

See Also

user, *modify*, *tmsh*

password-policy

Specifies the parameters of the valid passwords for the BIG-IP® system.

Syntax

Configure the **password-policy** component within the **auth** module using the syntax shown in the following sections.

Modify

```
modify password-policy
    expiration-warning [integer]
    max-duration [integer]
    max-login-failures [integer]
    min-duration [integer]
    minimum-length [integer]
    password-memory [integer]
    policy-enforcement [disabled | enabled]
    required-lowercase [integer]
    required-numeric [integer]
    required-special [integer]
    required-uppercase [integer]
```

Display

```
list password-policy
list password-policy
show running-config password-policy
show running-config password-policy
    all-properties
    non-default-properties
    one-line
```

Description

Users assigned a role of **Administrator** or **Resource Administrator** can modify a password policy for the BIG-IP system to enforce a company's security requirements by defining the parameters for valid passwords. Users assigned other roles can view password policies.

Examples

password-policy max-duration 90 min-duration 30 minimum-length 6 required-lowercase 2 required-uppercase 2 required-special 1 required-numeric 1 expiration-warning 5

Creates a password policy that specifies that passwords are valid for a maximum of **90** days and a minimum of **30** days. Also specifies that to be valid, a password must contain at least **6** characters, but not more than **10**

characters, including **2** lowercase alpha characters, **2** uppercase alpha characters, and **1** number. Additionally, this policy specifies that the system automatically warns users five days before their passwords expire.

list password-policy

Displays the password policy.

Options

- **expiration-warning**
  Specifies the number of days before a password expires. Based on this value, the BIG-IP system automatically warns users when their password is about to expire. The default value is **7** days.
- **max-duration**
  Specifies the maximum number of days a password is valid. The default value is **99999**.
- **max-login-failures**
  Specifies the number of consecutive unsuccessful login attempts that the system allows before locking out the user. The default value is **0** (zero - disabled).
- **min-duration**
  Specifies the minimum number of days a password is valid. The default value is **0** (zero).
- **minimum-length**
  Specifies the minimum number of characters in a valid password. The default value is **6**.
- **password-memory**
  Specifies whether the user has configured the BIG-IP system to remember a password on a specific computer. The default value is **0** (zero).
- **policy-enforcement**
  Enables or disables the password policy on the BIG-IP system. The default value is **disabled**.
- **required-lowercase**
  Specifies the number of lowercase alpha characters that must be present in a password for the password to be valid. The default value is **0** (zero).
- **required-numeric**
  Specifies the number of numeric characters that must be present in a password for the password to be valid. The default value is **0** (zero).
- **required-special**
  Specifies the number of special characters that must be present in a password for the password to be valid. The default value is **0** (zero).
- **required-uppercase**
  Specifies the number of uppercase alpha characters that must be present in a password for the password to be valid. The default value is **0** (zero).

See Also

user, *modify*, *tmsh*

radius

Configures a RADIUS configuration object for implementing remote RADIUS-based authentication of BIG-IP® system users.

Syntax

Configure the **radius** component within the **auth** module using the syntax shown in the following sections.

Create/Modify

```
create radius [name]
modify radius [name]
    accounting-bug [disabled | enabled]
    app-service [[string] | none]
    client-id [none | [string] ]
    debug [disabled | enabled]
    description [string]
    retries [integer]
    servers [add | delete | replace-all-with]
      { [ [hostname] | [ip address] ... ] }
    servers [default | none]
    service-type [default | login | framed | callback-login |
                  callback-framed | outbound | administrative |
                  nas-prompt | authenticate-only |
                  callback-nas-promit | call-check |
                  callback-administrative]
edit radius [ [ [name] | [glob] | [regex] ] ...]
     all-properties
     non-default-properties
```

Display

```
list radius
list radius [ [ [name] | [glob] | [regex] ] ...]
show running-config radius
show running-config radius [ [ [name] | [glob] | [regex] ] ...]
    all-properties
    non-default-properties
    one-line
    partition
```

Delete

```
delete radius [name]
```

Description

To authenticate BIG-IP system users when their authentication data is stored on a remote RADIUS server, you configure a RADIUS server, configure a RADIUS configuration object that references that RADIUS server, and then

activate RADIUS authentication for the BIG-IP system. In this case, client credentials are based on basic HTTP authentication (that is, user name and password).

To configure RADIUS authentication for the BIG-IP system:

1. Use the **radius-server** component in the **auth** module to configure a RADIUS server. For more information about creating a RADIUS server, see **help radius-server**.

2. Use the **radius** component in the **auth** module to create a RADIUS configuration object that references the RADIUS server you created in Step 1.

3. To activate RADIUS authentication for BIG-IP system users, type the following command sequence: **modify / auth source type radius**

Examples

create radius bigip_radius_auth servers add {myradiusserver}

Creates a RADIUS configuration object named **bigip_radius_auth**.

delete radius bigip_radius_auth

Deletes the RADIUS configuration component named **bigip_radius_auth**.

Options

- **accounting-bug**
  Enables or disables validation of the accounting response vector. This option is necessary only on older servers. The default value is **disabled**.
- **app-service**
  Specifies the name of the application service to which the RADIUS configuration object belongs. The default value is **none**. **Note:** If the **strict-updates** option is **enabled** on the application service that owns the object, you cannot modify or delete the RADIUS configuration object. Only the application service can modify or delete the RADIUS configuration object.
- **client-id**
  Sends a NAS-Identifier RADIUS attribute with string bar. If you do not specify a value for this option, the system uses the pluggable authentication module (PAM) service type. You can disable this feature by specifying a blank client ID.
- **debug**
  Enables or disables **syslog-ng** debugging information at the LOG DEBUG level. F5 Networks does not recommend this option for normal use. The default value is **disabled**.
- **description**
  User defined description.

- **glob**
  Displays the items that match the **glob** expression. See **help glob** for a description of **glob** expression syntax.
- **name**
  Specifies a unique name for the component. This option is required for the commands **create** and **modify**.
- **partition**
  Displays the partition within which the component resides.
- **regex**
  Displays the items that match the regular expression. The regular expression must be preceded by an at sign (@[regular expression]) to indicate that the identifier is a regular expression. See **help regex** for a description of regular expression syntax.
- **retries**
  Specifies the number of authentication retries that the BIG-IP local traffic management system allows before authentication fails. The default value is **3**.
- **service-type**
  Specifies the type of service used for the RADIUS server. The default is **default**, which behaves as **authenticate-only**.
- **servers**
  Specifies the host names or IP addresses of existing RADIUS servers that the BIG-IP system uses to obtain authentication data.

See Also

radius-server, *user*, *create*, *delete*, glob, *list*, *modify*, regex, *run*, *show*, *tmsh*

radius-server

Configures a RADIUS server for implementing remote RADIUS-based authentication of BIG-IP® system users.

Syntax

Configure the **radius-server** component within the **auth** module using the syntax shown in the following sections.

Create/Modify

```
create radius-server [name]
modify radius-server [name]
    app-service [[string] | none]
    description [string]
    port [ [name] | [number] ]
    secret [none | ["string"] ]
    server [ [hostname] | [IP address] | none]
    timeout [integer]
edit radius-server [ [ [name] | [glob] | [regex] ] ...]
    all-properties
    non-default-properties
```

Display

```
list radius-server
list radius-server [ [ [name] | [glob] | [regex] ] ...]
show running-config radius-server
show running-config radius-server [ [ [name] | [glob] | [regex] ] ...]
    all-properties
    non-default-properties
    one-line
    partition
```

Delete

```
delete radius-server [name]
```

Description

To authenticate BIG-IP system users when their authentication data is stored on a remote RADIUS server, you configure a RADIUS server, configure a RADIUS configuration object that references that RADIUS server, and then activate RADIUS authentication for the BIG-IP system. In this case, client credentials are based on basic HTTP authentication (that is, user name and password).

To configure RADIUS authentication for the BIG-IP system:

1. Use the **radius-server** component in the **auth** module to configure a RADIUS server.

2. Use the **radius** component in the **auth** module to create a RADIUS configuration object that references the RADIUS server you created in the Step 1. For more information about creating a RADIUS configuration object, see **help radius**.

3. To activate RADIUS authentication for BIG-IP system users, type the following command sequence: **modify / auth source type radius**

Examples

create radius-server bigip_auth_radius_server secret "This is the secret." server 10.1.1.1

Creates a RADIUS server component named **bigip_auth_radius_server**.

delete radius-server bigip_auth_radius_server

Deletes the RADIUS server component named **bigip_auth_radius_server**.

Options

- **app-service**
  Specifies the name of the application service to which the RADIUS server belongs. The default value is **none**. **Note:** If the **strict-updates** option is **enabled** on the application service that owns the object, you cannot modify or delete the RADIUS server. Only the application service can modify or delete the RADIUS server.
- **description**
  User defined description.
- **glob**
  Displays the items that match the **glob** expression. See **help glob** for a description of **glob** expression syntax.
- **name**
  Specifies a unique name for the component. This option is required for the commands **create** and **modify**.
- **partition**
  Displays the partition in which the radius server resides.
- **port**
  Specifies the port for RADIUS authentication traffic. The default value is **1812**.
- **regex**
  Displays the items that match the regular expression. The regular expression must be preceded by an at sign (@[regular expression]) to indicate that the identifier is a regular expression. See **help regex** for a description of regular expression syntax.
- **secret**
  Specifies the secret key the system uses to encrypt and decrypt packets sent from or received by the server. This option is required.

- **server**
  Specifies the host name or IP address of the RADIUS server. This option is required.
- **timeout**
  Specifies the timeout value in seconds. The default value is **3**.

See Also

radius, *user*, *create*, *delete*, glob, *list*, *modify*, regex, *run*, *show*, *tmsh*

remote-role

Creates remote role information in a file that an LDAP, Active Directory®, RADIUS, or TACACS+ server reads to determine the specific access rights to grant to groups of remotely-authenticated users.

Syntax

Configure the **remote-role** component within the **auth** module using the syntax shown in the following sections.

Modify

```
modify remote-role
  description [string]
  role-info [add | delete | modify | replace-all-with] {
   [group-name] {
     attribute [string]
     console [disabled | tmsh]
     description [string]
     deny [enabled | disabled]
     line-order [integer]
     role [acceleration-policy-editor | admin | fraud-protection-manager |
           application-editor | auditor | certificate-manager |
           firewall-manager | guest | irule-manager | manager |
           no-access | operator | resource-admin | user-manager |
           web-application-security-administrator |
           web-application-security-editor]
     user-partition [all | Common | [name] ]
     user-partition [%string]
   }
  }
  role-info none
```

Display

```
list remote-role
show running-config remote-role
    all-properties
    non-default-properties
    one-line
```

Delete

You cannot delete the remote-role defaults, you can only modify the values of the options.

Description

You can use the **remote-role** component to grant access to a specific group of remotely-authenticated users without creating a local user account on the BIG-IP® system for each user in the group.

Users assigned the role of **Administrator** or **Resource Administrator** can modify remote roles. Users assigned all other roles can view remote roles.

You can use the variable substitution feature to assign access rights for a group of remote users by specifying a text string variable that is preceded by a leading % character for the options **attribute**, **console**, **role** and **user-partition**. For example, if you define the remote role for the groups DC1 and DC2 as follows:

```
remote-role {
 role info {
   dc1 {
     attribute "F5-LTM-User-Info-1=DC1"
     console %F5-LTM-User-Console
     line-order 1
     role %F5-LTM-User-Role
     user-partition %F5-LTM-User-Partition
   }
   dc2 {
     attribute "F5-LTM-User-Info-1=DC2"
     line-order 2
   }
  }
}
```

The BIG-IP® system attempts to match the value of the **attribute** option, **F5-LTM-User-Info-1=DC1**, and then pulls the value of the **console**, **role** and **user-partition** options from the other variables.

◆ Note

If a variable includes an incorrect value, the system does not authorize the user. Additionally, if you have not defined the variables, as with the group DC2 above, the system authenticates the user with the following access rights:

- console = disabled
- role = none
- user-partition = none

Examples

modify remote-role role-info add { my_managers { attribute "memberOF=cn=BigIPmanagerGroup,cn=users,dc=mydept,dc=mycompany,dc=com" console disabled line-order 1000 role 100 user-partition all } }

Configures a remote role, named **my_managers**, for LDAP authentication, by creating the 1000th line of the **/config/bigip/auth/remoterole** file, and granting the Manager role (**100**) in all partitions to the remote users assigned this role.

modify remote-role role-info add { my_admins { attribute "NS-Admin-Privilege" console tmsh line-order 1000 role 0 user-partition all } }

Configures a remote role, named **my_admins**, for LDAP authentication, by creating the 2000th line of the **/config/bigip/auth/remoterole** file, and granting the Administrator role (**0**) in all partitions to the remote users assigned this role.

modify remote-role role-info add { my_managers { attribute "manager_group=manager" console tmsh line-order 3000 user-partition all } }

Configures a remote role, named **my_managers**, for RADIUS or TACACS+ authentication, by creating the 3000th line of the **/config/bigip/auth/remoterole** file, and granting the Administrator role (**0**) in all partitions to the remote users assigned this role:

Options

- **description**
  Specifies a user-defined description.
- **role-info**
  Configures the access rights for a specific group of remotely-authenticated users. You can configure the following information for a role:
  - **attribute**
    Specifies an attribute-value pair that an authentication server supplies to the BIG-IP system to match against entries in **/config/bigip/auth/remoterole**. The specified pair typically identifies users with access rights in common. This option is required. Alternatively, you can use the variable substitution feature (described in the Description section above), and specify a text string variable that is preceded by a leading % character.
  - **console**
    Enables or disables console access for the specified group of remotely-authenticated users. The default value is **disabled**. When using variable substitution, as described in the Description section of this man page, the variable for the **role** option must be: **tmsh**. If it does not the **console** option is **disabled**.
  - **deny**
    Enables or disables remote access for the specified group of remotely-authenticated users. The default value is **disabled**.
  - **description**
    Specifies a user-defined description.
  - **group-name**
    Specifies the name of the remote role that you are configuring. This option is required.

- **line-order**
  Specifies the number of the first populated line in the file, **/config/bigip/auth/remoterole**. The LDAP, Active Directory, RADIUS, and TACACS+ servers read this file line by line. The order of the information is important; therefore, F5 Networks recommends that you set the first line at **1000**. This allows you, in the future, to insert lines before the first line. This option is required.
- **role**
  Specifies the role that you want to grant to the specified group of remotely-authenticated users. The default value is **no-access**. The available roles are:

admin

fraud-protection-manager

application-editor

certificate-manager

firewall-manager

guest

manager

no-access

operator

resource-admin

web-application-security-administrator

web-application-security-editor

user-manager

When using variable substitution, as described in the Description section above, the variable for the **role** option must evaluate to one of these values: **0** (admin), **20** (resource admin), **40** (user manager), **80** (auditor), **100** (manager), **300** (application editor), **350** (advanced operator), **400** (operator), **450** (firewall manager), **500** (certificate manager), **510** (irule manager), **700** (guest), **800** (web application security administrator), **810** (web application security editor), **850** (acceleration policy editor), **900** (no-access).

- **user-partition**
  Specifies the user partition to which you are assigning access to the specified group of remotely-authenticated users. The default value is **Common**. This option is required.
  Alternatively, you can use the variable substitution feature (described in the Description section above) and specify a text string variable that is preceded by a leading % character.

See Also

remote-user, *user*, *list*, *modify*, *show*, *tmsh*

remote-user

Configures the default role, partition access, and console access for all remotely authenticated user accounts that have not been added as local user accounts on the BIG-IP® system.

Syntax

Configure the **remote-user** component within the **auth** module using the syntax shown in the following sections.

Modify

```
modify remote-user
    default-partition [all | Common | [partition name] ]
    default-role [acceleration-policy-editor | admin |
                  fraud-protection-manager | application-editor |
                  auditor | firewall-manager | guest |
                  irule-manager | manager | no-access |
                  operator | resource-admin | user-manager |
                  web-application-security-administrator |
                  web-application-security-editor ]
    description [string]
    remote-console-access [disabled | tmsh]
```

Display

```
list remote-user
show running-config remote-user
    all-properties
    non-default-properties
    one-line
```

Delete

You cannot delete the **remote-user** defaults, you can only modify the values of the options.

Description

You can use the **remote-user** component to configure the default parameters for all the remote user accounts on the BIG-IP system as a group. To assign a different access level to a specific remote user, you must create a local user account for that user on the BIG-IP system. See the **auth user** man page for more information.

Users assigned the role of Administrator or Resource Administrator can modify the parameters of the **remote-user** component. Users assigned all other roles can view the parameters of the **remote-user** component.

Examples

modify remote-user default-partition Common default-role no access remote-console-access disabled

For all remote users, sets the default partition access to partition **Common**, the default role to **no-access**, and the default remote console access to **disabled**.

modify remote-user default-partition all default-role no access remote-console-access disabled

For all remote users, sets the default partition access to **all** partitions, the default role to **no-access**, and the default remote console access to **disabled**.

Options

- **default-partition**
  Specifies the default partition for all remote user accounts. The default value is **all**.
- **default-role**
  Specifies the default role for all remote user accounts. The default value is **no-access**.
- **description**
  Specifies a user-defined description.
- **remote-console-access**
  Specifies whether you are granting this user access to **tmsh** or disabling remote console access for this user. The default value is **disabled**.

See Also

remote-role, *user*, *list*, *modify*, *show*, *tmsh*

source

Configures the authorization source type for a BIG-IP® system.

Syntax

Configure the **source** component within the **auth** module using the syntax in the following sections.

Modify

```
modify source
    type [active-directory | ldap | local | radius | tacacs | cert-ldap | apm-auth]
```

Display

```
list source
list source [option]
    all-properties
    non-default-properties
    one-line
```

Description

You can use the **source** component to set up the authorization source type for the BIG-IP system.

Examples

modify auth source type tacacs

Sets up the authorization source type as **tacacs**.

list auth source type

Displays the authorization source type.

Options

- **type**
  Specifies the default user authorization source. The default value is **local**. When user accounts that access the system reside on a remote server, the value of the this option is the type of server that you are using for authentication, for example, **ldap**.

See Also

list, *modify*, *tmsh*

tacacs

Configures a TACACS+ configuration object for implementing remote authentication of BIG-IP® system users based on TACACS+.

Syntax

Configure the **tacacs** component within the **auth** module using the syntax shown in the following sections.

Create/Modify

```
create tacacs [name]
modify tacacs [name]
    accounting [send-to-first-server | send-to-all-servers]
    app-service [[string] | none]
    authentication [use-first-server | use-all-servers]
    debug [disabled | enabled]
    description [string]
    encryption [disabled | enabled]
    protocol [none | [protocol] ]
    secret [ "[string]" ]
    servers
      [add | delete | replace-all-with] {
        [ [hostname] | [ip address] ] ...
    }
    service [ [name] | none]
edit tacacs [ [ [name] | [glob] | [regex] ] ...]
      all-properties
      non-default-properties
```

Display

```
list tacacs
list tacacs [ [ [name] | [glob] | [regex] ] ...]
show running-config tacacs
show running-config tacacs [ [ [name] | [glob] | [regex] ] ...]
    all-properties
    non-default-properties
    one-line
    partition
```

Delete

```
delete tacacs [name]
```

Description

To authenticate BIG-IP system users when their authentication data is stored on a remote TACACS+ server, you create a TACACS+ configuration object, and then activate the object.

To configure TACACS+ authentication for BIG-IP system users:

1. Use the **tacacs** component in the **auth** module to configure a TACACS+ configuration object.

2. To activate TACACS+ authentication for BIG-IP system users, run the following command sequence: **modify / auth source type tacacs**

Examples

create tacacs bigip_tacacs_auth servers add {my_tacacs_server}

Creates a TACACS+ configuration object named **bigip_tacacs_auth**.

delete tacacs bigip_tacacs_auth

Deletes the TACACS+ configuration object named **bigip_tacacs_auth**.

Options

- **accounting**
  If multiple TACACS+ servers are defined and pluggable authentication module (PAM) session accounting is enabled, sends accounting start and stop packets to the first available server or to all servers. The default value is **send-to-first-server**.
  Possible values are:
  - **send-to-all-servers**
    The system sends accounting start and stop packets to all servers.
  - **send-to-first-server**
    The system sends accounting start and stop packets to the first available server.
- **app-service**
  Specifies the name of the application service to which the TACACS+ configuration object belongs. The default value is **none**. **Note:** If the **strict-updates** option is **enabled** on the application service that owns the object, you cannot modify or delete the TACACS+ configuration object. Only the application service can modify or delete the TACACS+ configuration object.
- **authentication**
  Specifies the process the system employs when sending authentication requests. The default value is **use-first-server**.
  Possible values are:
  - **use-all-servers**
    The system sends an authentication request to each server until authentication succeeds, or until the system has sent a request to all servers in the list.
  - **use-first-server**
    The system sends authentication requests to only the first server in the list.

- **debug**
  Enables **syslog-ng** debugging information at the LOG DEBUG level. F5 Networks does not recommend this option for normal use. The default value is **disabled**.
- **description**
  User defined description.
- **encryption**
  Enables or disables encryption of TACACS+ packets. F5 Networks recommends this option for normal use. The default value is **enabled**.
- **glob**
  Displays the items that match the **glob** expression. See **help glob** for a description of **glob** expression syntax.
- **name**
  Specifies a unique name for the component. This option is required for the commands **create** and **modify**.
- **partition**
  Displays the administrative partition within which the component resides.
- **protocol**
  Specifies the protocol associated with the value specified in the **service** option, which is a subset of the associated service being used for client authorization or system accounting.
- **regex**
  Displays the items that match the regular expression. The regular expression must be preceded by an at sign (@[regular expression]) to indicate that the identifier is a regular expression. See **help regex** for a description of regular expression syntax.
- **secret**
  Sets the secret key used to encrypt and decrypt packets sent or received from the server. This option is required.
- **servers**
  Specifies the host name or IP address of the TACACS+ server. This option is required.
- **service**
  Specifies the name of the service that the user is requesting to be authenticated to use. Identifying the service enables the TACACS+ server to behave differently for different types of authentication requests. This option is required.

See Also

user, *create*, *delete*, *edit*, glob, *list*, *modify*, regex, *run*, *show*, *tmsh*

user

Configures user accounts for the BIG-IP® system.

Syntax

Modify the **user** component within the **auth** module using the syntax shown in the following sections.

Create/Modify

```
create user [name]
modify user [name]
    description [text...]
    partition-access [add | modify | delete |replace-all-with { [partition-name] {
role [role-name] } } ]
    password [text]
    prompt-for-password
    shell [name]
```

where [role-name]: [acceleration-policy-editor | admin | fraud-protection-manager | application-editor | auditor | certificate-manager | firewall-manager | guest | irule-manager | manager | no-access | operator | resource-admin | user-manager | web-application-security-administrator | web-application-security-editor]

Display

```
list user
list user [ [ [name] | [glob] | [regex] ] ... ]
show running-config user
show running-config user [ [ [name] | [glob] | [regex] ] ... ]
    encrypted-password
    one-line
    partition
show user
    field-fmt
```

Delete

```
delete user [name]
```

Description

You can create user accounts where the user names differ only by case-sensitivity (for example, david and DAVID).

You can configure the partition-access property to grant a user access to more than one partition on the system. In the case where you do not grant the user access to all partitions, you can assign the user a different user role for each partition. A user can have only one role per partition. Any user with

a role of **Administrator**, **Resource Administrator**, **Web Application Security Administrator**, or **Auditor** always has access to all partitions and can have no other role on the system.

Only users with the **Administrator** or **User Manager** roles are allowed to create or modify user accounts.

Additionally, only users with the **Administrator**, **Resource Administrator**, or **User Manager** user role can view all of the user accounts in all of the partitions to which the user has access. Therefore, if you have a user role other than one of these roles, you can only view your own user account.

Examples

create user nwinters partition-access add { all-partitions { role guest } }

Creates a new user named **nwinters** with a role of **Guest** in all partitions.

create user tknox password aBcD007 partition-access add { partition1 { role operator } }

Creates a new user named **tknox** with a role of **operator** in partition named partition1 and sets the user's login password.

list user

Displays the viewable properties of all user accounts.

show user

Displays each user role and the corresponding partition access that is currently assigned to the user.

Options

- **description**
  Describes the user account in free form text.
- **encrypted-password**
  Displays the encrypted password for the user account.
- **glob**
  Displays the items that match the **glob** expression. See **help glob** for a description of **glob** expression syntax.
- **name**
  Specifies a unique name for the component. This option is required for the commands **create** and **modify**.

◆ Note

User account names are case-sensitive.

- **partition**
  Displays the name of the administrative partition in which the user account resides.

- **partition-access**
  Specifies the administrative partitions to which the user currently has access. Note that in addition to these partitions, the user also has read access to the shared partitions Common and Root. An exception to this is any user with the role **No Access**.
- **role**
  Specifies the user role that pertains to the partition specified by the partition-access property. If you do not want to assign a user role to the user account, specify the value **no-access**. This pevents the user from accessing the system.
- **password**
  Sets the user password during creation or modification of a user account without prompting or confirmation. May not be used with prompt-for-password. Passwords are hidden in log and history files.
- **prompt-for-password**
  Indicates that when the account is created or modified, the BIG-IP system prompts the administrator or user manager for both a password and a password confirmation for the account.
- **regex**
  Displays the items that match the regular expression. The regular expression must be preceded by an at sign (@[regular expression]) to indicate that the identifier is a regular expression. See **help regex** for a description of regular expression syntax.
- **shell**
  Specifies the shell to which the user has access. Valid values are:
  - **bash**
    Provides an unrestricted system prompt. You can assign access to the **bash** shell only to users with the **Administrator** or **Resource Administrator** role. However, F5 Networks recommends that you do not give **bash** shell access to users with the **Resource Administrator** user role unless they use the **tcpdump**, **ssldump**, or **qkview** utilities, or if they manage certificate and key files using the console. Instead, F5 Networks recommends that you give these users **tmsh** access.
  - **none**
    Specifies no shell access. The user must use the Configuration utility.
  - **tmsh**
    Provides access to the Traffic Management shell.

See Also

partition, *password*, *create*, *delete*, *list*, *modify*, *show*, *tmsh*

43

cli

- Introducing the cli module
- Alphabetical list of components

Introducing the cli module

You can use the tmsh components that reside within the cli module to configure administrative partitions, aliases, and the command line preferences. For more information about the tmsh hierarchical structure, see Chapter 2, *Understanding and Using the Traffic Management Shell*.

Alphabetical list of components

The remainder of this chapter lists the tmsh components that are available in the cli module.

admin-partitions

Set the administrative partition for a BIG-IP® configuration file.

Syntax

Configure the **admin-partitions** component within the **cli** module using the syntax in the following sections.

Modify

```
admin-partitions
    update-partition [name]
```

Description

You can use the **admin-partitions** component to set the administrative partition in which configuration will be loaded when a configuration file is being loaded.

This component is only available from a configuration file that is being loaded via the **sys config** component with the **file** option.

Examples

cli admin-partitions { update-partition partition_A }

Sets the administrative partition in which configuration will be loaded. Configuration that follows this directive will be place in partition_A.

Options

- **update-partition**
  Sets the administrative partition in which you can configure objects.

See Also

load, *config*, *tmsh*

global-settings

Configures settings for tmsh

Syntax

Configure the **global-settings** component within the **cli** module using the syntax shown in the following sections.

Modify

```
edit global-settings
    all-properties
    non-default-properties
modify global-settings
    audit [disabled | enabled]
    description [string]
    idle-timeout [disabled | integer]
    scf-backup-number [integer]
    service [number | name]
```

Display

```
list global-settings
list global-settings [option]
    all-properties
    non-default-properties
    one-line
```

Delete

You cannot delete the default global settings.

Description

You can use the **global-settings** component to configure multiple settings for **tmsh**.

Examples

modify global-settings audit enabled

Enables auditing for **tmsh**.

modify global-settings idle-timeout 15

Sets the user idle timeout from **tmsh** to 15 minutes.

Options

- **audit**
  Specifies the global audit level for **tmsh**. The audited commands are stored in **/var/log/audit**. The default value is **enabled**. The audit levels are:
  - **disabled**
    tmsh does not log commands that users enter.
  - **enabled**
    tmsh audits only commands that users enter. Note that the system does not audit the commands that the command **load** runs.
- **description**
  User defined description.
- **idle-timeout**
  If not **disabled**, log a user in tmsh interactive mode out automatically after a specified set of minutes. An administrator may change the timeout value at any time and the new policy will take place immediately.
- **scf-backup-number**
  Specifies the number of backup single configuration files that the system stores when you enter the following command sequence in **tmsh**:
  load sys config file
  When you run the command, the system saves the single configuration file. By default, the system saves two backup single configuration files. For example, if you set the **scf-backup-number** option to **3**, after you run the command sequence **tmsh load sys config file** for the third time, the system has three versions of the single configuration file: **/var/local/scf/backup.scf**, **/var/local/scf/backup-1.scf**, and **/var/local/scf/backup-2.scf**. The newest file is **/var/local/scf/backup.scf**.
- **service**
  Specifies the format in which **tmsh** displays a service. The default value is **name**. The options are:
  - **name**
    Displays a service using a protocol name, for example, **http**.
  - **number**
    Displays a service using a numeric value, for example, **192.168.10.20:80**, where 80 indicates http.

See Also

edit, *list*, *modify*, *run*, *tmsh*

history

Displays a list of commands in the order in which you ran the commands.

Syntax

Use the **history** component within the **cli** module to display a numbered list of commands in the order the commands were issued.

Display

```
show history
!
!!
![string]
```

Description

You can use the **history** component to display a numbered list of the commands that you have run in **tmsh**. The commands display in the order in which you ran the commands, and each command is identified by an entry ID. The larger the entry ID of the command, the more recently you ran the command.

To rerun a command from the history list, type **q** to close the list and return to the **tmsh** prompt, and then enter an exclamation point (**!**) followed by the entry ID of the command that you want to run.

Examples

!

show history

Either of the two previous commands, displays the command history list.

!5

Runs the fifth command in the command history list.

!!

Runs the previously issued command.

!create

Runs the last command that begins with **create**.

See Also

show, *tmsh*

preference

Configures **tmsh** preferences.

Syntax

Configure the **preference** component within the **cli** module using the syntax shown in the following sections.

Modify

```
edit preference
modify preference [option]
    alias-path [string list]
    app-service [[string] | none]
    confirm-edit [disabled | enabled]
    display-threshold [integer]
    editor [nano | vi]
    history-date-time [disabled | enabled]
    history-file-size [integer]
    history-size [integer]
    keymap [default | emacs | vi]
    list-all-properties [disabled | enabled]
    pager [disabled | enabled]
    prompt { [avc-count config-sync-status current-folder
              fully-qualified-host host mcp-load-status
              mcp-state multi-line status user user-role] | none }
    show-aliases [disabled | enabled]
    stat-units [default | exa | gig | kil | meg | peta | raw |
                tera | yotta | zetta]
    suppress-warnings [ all | config-version | none ]
    table-indent-width [integer]
    tcl-syntax-highlighting [disabled | enabled]
    video [disabled | enabled]
    warn [bell | disabled | visual-bell]
edit preference
    all-properties
```

Display

```
list preference
list preference [option]
show running-config preference
show running-config preference [option]
    all-properties
    one-line
```

Description

You can use the **preference** component to configure **tmsh** to meet your specific needs.

Examples

modify preference display-threshold 500

Configures **tmsh** to retrieve up to **500** objects before requiring a user response to the question, **"Display all items? (y/n)."**

modify preference history-file-size 80

Configures the maximum number of commands that a user can view in the command history list to be **80**.

modify preference history-size 1000

Configures the maximum number of commands that **tmsh** saves in a user's **.tmsh_history** file to be **1000** commands.

modify preference suppress-warnings config-version

Configures **tmsh** to suppress warning messages for configuration version related (for backward compatibility of configuration).

Options

- **alias-path**
  Specifies the search paths for shared aliases. The shared aliases could be in multiple locations, only ones on the search paths can be used. If a folder is deleted from the system it will be automatically remove from the alias-path.
- **app-service**
  Specifies the name of the application service to which the **preference** belongs. The default value is **none**. **Note:** If the **strict-updates** option is **enabled** on the application service that owns the object, you cannot modify or delete the **preference**. Only the application service can modify or delete the **preference**.
- **confirm-edit**
  Specifies whether the command **edit** prompts for confirmation before saving changes. The default value is **enabled**.
  Note that the value of this option does not affect the behavior of the editor if the changes made in the editor result in a failed update. In this case, **tmsh** always prompts the user to either re-edit the file or discard the changes. The options are:
  - **enabled**
    tmsh prompts a user to either submit (y), discard (n), or edit (e) the changes made to a component within the editor.
  - **disabled**
    tmsh does not prompt the user, but instead, immediately submits the changes made in the editor.
- **display-threshold**
  Specifies the maximum number of objects that **tmsh** displays without requiring a user response to the question, **"Display all [number] items?**

(y/n)." You can specify from **0** (zero) through **4,294,967,265** objects. If you set this option to **0** (zero), **tmsh** displays an unlimited number of objects without requesting a response.

- **editor**
  Specifies the editor that the command **edit** invokes. Users assigned the user role of **Administrator** can select **nano** or **vi**. Users assigned other user roles must use **nano**.
- **history-date-time**
  Specifies whether **tmsh** displays in the command history the date and time that each command was issued. The default value is **disabled**. Note that the command history file, **~/.tmsh-history-[user]**, always contains the date and time that a command was issued.
- **history-file-size**
  Specifies the maximum number of **tmsh** commands that the system saves in each user's **.tmsh_history** file. If you set this option to **0** (zero), the system does not save **tmsh** commands in the file. The maximum value is **100,000**. For performance reasons, the system does not truncate the file after a user enters a command. Instead, the system truncates the file after a user exits **tmsh**.
- **history-size**
  Specifies the number of commands that a user can view or search in the command history list. The maximum number of commands is **100,000**. The default value is **500**.
  If you set this option to **0** (zero), the system does not add commands to the list of commands in memory; however, the system does write commands to the **.tmsh_history** file, unless the **history-file-size** option is set to **0** (zero).
  When you change the value of this option, the system renumbers the commands listed in memory; however, the commands remain in the same order.
- **keymap**
  Specifies the keyboard bindings that you want **tmsh** to use. The default value is **default**. The options are **default**, **emacs**, and **vi**.
- **list-all-properties**
  Specifies whether the system displays all of the properties of a component by default when you run the command **list**. The default value is **disabled**.
- **pager**
  Specifies whether the system sends the output of the **tmsh** commands **list** and **show** to **less**. The default value is **enabled**.
- **prompt**
  Specifies the information that you want to display in the **tmsh** prompt. By default the prompt displays **user_name@host_name(tmos-current_module)#**. The options are:

- **avc-count**
  Displays the current SELinux Access Vector Cache in the **tmsh** prompt. The value displayed in the prompt indicates the number of times SELinux has denied access to a protected resource. The default is to not display this information.
- **config-sync-status**
  Displays global sync status in the **tmsh** prompt. The status displayed in the prompt indicates the rolled-up sync status of all the device groups where the local device resides. The default is to display this information.
- **current-folder**
  Displays the current working folder in the **tmsh** prompt. The default is to not display this information.
- **fully-qualified-host**
  Displays the fully qualified host name in the **tmsh** prompt. The default is to not display this information.
- **host**
  Displays the host name in the **tmsh** prompt. The default is to display the host name in the prompt.
- **mcp-load-status**
  Displays the configuration file load status in the **tmsh** prompt. This information is also available in the **Last Configuration Load Status** of the **show sys mcp** command output. The default is to not display this information.
- **mcp-state**
  Displays the running phase of the mcpd service in the **tmsh** prompt. This information is also available in the **Running Phase** of the **show sys mcp** command output. The default is to not display this information.
- **multi-line**
  Displays the **tmsh** prompt on multiple lines, with information on the first line, and a pound sign (#) on the second line, for example:
  (Common:all) operator1@6400(tmos.cli)
  #
  The **multi-line** option is disabled by default.
- **none**
  Sets the **tmsh** prompt to display **(tmos.current_module)#**, where the system replaces **current_module** with the name of the module within which you are working.
- **status**
  Displays the system status in the **tmsh** prompt. The default is to display system status in the prompt.
- **user**
  Displays the user name in the **tmsh** prompt. The default value is to display the user name in the prompt.
- **user-role**
  Display the user's current role in the **tmsh** prompt. By default the user role is not displayed in the prompt.

- **show-aliases**
  Specifies whether the system displays aliases in the results of the command completion and context-sensitive help features. The default value is **enabled**.
- **suppress-warnings**
  Specifies the type of warning messages which needs to be suppressed. The default value is **none**.
- **stat-units**
  Specifies the default unit in which the system displays statistics. The options are:
  - **default**
    Displays data in the simplest units. For example, if the value of the data is 1,200,001, the system displays 1.20M; however, if the value of the data is 1,200, the system displays 1.2K.
  - **exa**
    Display data in parts per quintillion.
  - **gig**
    Displays data in parts per billion.
  - **kil**
    Displays data in parts per thousand.
  - **meg**
    Displays data in parts per million.
  - **peta**
    Displays data in parts per quadrillion.
  - **raw**
    Displays raw data.
  - **tera**
    Displays data in parts per trillion.
  - **yotta**
    Displays data in parts per septillion.
  - **zetta**
    Displays data in parts per sextillion.
- **table-indent-width**
  Specifies the indent width when **tmsh** displays the child object tables in a show command. You can specify from **0** (zero) through **10**. If you set this option to **0** (zero), **tmsh** displays child object tables without any indent.
- **tcl-syntax-highlighting**
  Specifies whether Tcl syntax highlighting will be enabled in the editor. This setting only applies if your **editor** preference is set to **vi**. The default value is **disabled**.
- **video**
  Enables or disables any video features used to highlight text. The default value is **enabled**.

- **warn**
  Specifies how the system warns you when you make an incorrect keystroke. The default value is **bell**.
  The options are:
  - **bell**
    Sounds a bell.
  - **disabled**
    Disables the warning function.
  - **visual-bell**
    Displays a visual warning.

See Also

edit, *list*, *modify*, *show*, *mcp-state*, *tmsh*

script

Automates **tmsh** using Tool Command Language (Tcl).

Syntax

Configure the **script** component within the **cli** module using the syntax shown in the following sections.

Edit

```
create script [name]
modify script [name]
  app-service [[string] | none]
  description [string]
  ignore-verification [true | false]
  script-checksum [[string] | none]
  script-signature [[string] | none]
edit script [ [ [name] | [glob] | [regex] ] ... ]
  all-properties
```

Display

```
list script
list script [ [ [name] | [glob] | [regex] ] ... ]
show running-config script
show running-config script [ [ [name] | [glob] | [regex] ] ... ]
  all-properties
```

Delete

```
delete script [name]
```

Generate

◆ Note

generate cryptographic signature or checksum based on cli script text.

```
generate cli script [name]
    checksum
    signature
```

Run

```
run script [name] [options ...]
    file [file name] [options ...]
    verbatim-arguments [file option] [file name] [options ...]
```

The options that are available depend on which script you are running.

The **file** option is limited to users with the role of **administrator**.

Description

You can use the **script** component to build Tcl scripts to automate management of the BIG-IP® system. By combining command aliases with scripts, you can extend **tmsh** to build commands that are customized to your environment.

To do this, place the content of the script inside one or more Tcl procedures. The content of a script cannot exceed 65,000 bytes. However, a script can include other scripts. For more information about including scripts in other scripts, see **tmsh::include** following.

Starting with BIGIP 11.5.0, tmsh commands are versioned. the tmsh active version should be specified in scripts. This will avoid breaking scripts due to changes in tmsh syntax in the different versions. See examples below for how to use it in a script. Without tmsh active version specified, scripts will run on the current active version. By default, the active version will be the latest cli version.

You can use the following procedures in the manner specified:

- **script::run**
  tmsh invokes the procedure **script::run** when you issue the command sequence **run / cli script [name]**. A script is run relative to the module in which the **run** command is invoked.
  The **script::run** procedure must be defined in the script named by the **run** command. Scripts that are included by **tmsh::include** are not required to implement the procedure **script::run**.
- **script::help**
  Provides context sensitive help. A script is not required to implement **script::help**.
- **script::tabc**
  Provides context sensitive help. A script is not required to implement **script::tabc**.
- **script::init**
  tmsh calls the procedure **script::init** before calling one of the following procedures: **script::run**, **script::help**, or **script::tabc**. The **script::init** procedure can use the Tcl variable **tmsh::csh** to determine which one of these three procedures **tmsh** invokes after **tmsh:init**.
  Additionally, you can use the procedure **script::init** to initialize global variables. A script is not required to implement **script::init**.

Examples

edit script myscript

Creates or modifies the script **myscript**.

edit script myscript yourscript

Creates or modifies the scripts **myscript** and **yourscript** at the same time.

list script myscript

Displays the contents of the script **myscript**.

delete script [name]

Deletes the script **myscript** from the system.

run script myscript [arguments ...]

Runs the script **myscript**. The system passes arguments to the script in the following Tcl variables:

- **tmsh::argc** contains the number of arguments including the name of the script.
- **tmsh::argv** contains the list of argument values. The first item in **tmsh::argv** is always the name of the script.

Tip: You can create an alias for the command sequence **run / cli script [name]** using the **cli alias** component. For more information, see **help cli alias**.

run script verbatim-arguments myscript [arguments ...]

Runs the same commands as **run script myscript [arguments...]** above, except the system passes all arguments specified in the command as one argument to the script. Note that you do not need to enclose the argument list in double quotes, and you do not need to escape special characters.

generate my_script checksum

Generate a checksum for the script text and add the checksum as a property.

generate my_script signature signing-key my_key

Generate a signature for the script text using the specified private key and add the signature as a property.

Note: For a script which includes a checksum or signature to succesfully load,
the script text contents must match the stored checksum or signature.
To temporarily stop the verification of signature or checksum and still retain the checksum or
signature, the **ignore-verification** attribute must be set to **true**. This is done by editing the script and adding the **ignore-verification** attribute.

To completely clear the signature or checksum, simply set the attribute **script-signature** or
script-checksum to empty string "". By doing so, the script will be processed as if it was
never signed or checksumed.

```
modify script /Common/my_script {
proc script::init {} {
}

proc script::run {} {
}

proc script::help {} {
}
```

```
proc script::tabc {} {
}
   ignore-verification true
   script-checksum 74778e7b13016e0b9329a17f8d2da601
   total-signing-status checksum
   verification-status checksum-verified
}
```

Options

- **app-service**
  Specifies the name of the application service to which the object belongs. The default value is **none**. **Note:** If the **strict-updates** option is **enabled** on the application service that owns the object, you cannot modify or delete the object. Only the application service can modify or delete the object.
- **checksum**
  Generate a checksum for the script text and add the checksum to the script as a property. Only for use with the **generate** command.
- **description**
  A user defined description.
- **file**
  Specifies that the script to be run should come from a file located on the file system rather than a script from the configuration.
- **glob**
  Displays the scripts that match the **glob** expression. See **help glob** for a description of **glob** expression syntax.
- **name**
  Specifies a unique name for the script. This option is required for the **edit** and **delete** commands.
- **regex**
  Displays the scripts that match the regular expression. The regular expression must be preceded by an at sign (@[regular expression]) to indicate that the identifier is a regular expression. See **help regex** for a description of regular expression syntax.
- **signature**
  Generate a signature for the script text using the specified private key and add the signature to the script as a property. Only for use with the **generate** command.
- **signing-key**
  The private key to use for signing the script. Only for use with the **signature** option.
- **verbatim-arguments**
  Specifies that the arguments at the end of the command should not be tokenized by tmsh prior to being sent to the script. This is useful when the script is wrapping another utility that takes arguments.

Configuration And Status Accessors

The following Tcl commands mirror **tmsh** commands. For example, the Tcl **tmsh::create** command accepts the same components, object identifiers, and properties that the **tmsh create** command accepts.

- **tmsh::cd [args...]**
  Runs the **cd** command using the specified arguments.
- **tmsh::cp [args...]**
  Runs the **cp** command using the specified arguments.
- **tmsh::create [args...]**
  Runs the **create** command using the specified arguments.
- **tmsh::delete [args...]**
  Runs the **delete** command using the specified arguments.
- **tmsh::install [args...]**
  Runs the **install** command using the specified arguments.
- **tmsh::generate [args...]**
  Runs the **generate** command using the specified arguments.
- **tmsh::list [args...]**
  Runs the **list** command using the specified arguments. The system returns the results as a string.
- **tmsh::load [args...]**
  Runs the **load** command using the specified arguments.
- **tmsh::modify [args...]**
  Runs the **modify** command using the specified arguments.
- **tmsh::publish [args...]**
  Runs the **publish** command using the specified arguments.
- **tmsh::pwd**
  Runs the **pwd** command.
- **tmsh::reset-stats [args...]**
  Runs the **reset-stats** command using the specified arguments.
- **tmsh::restart [args...]**
  Runs the command **restart** using the specified arguments.
- **tmsh::run [args...]**
  Runs the **run** command using the specified arguments.
- **tmsh::save [args...]**
  Runs the **save** command using the specified arguments.
- **tmsh::show [args...]**
  Runs the **show** command using the specified arguments. The system returns the results as a string.
- **tmsh::start [args...]**
  Runs the command **start** using the specified arguments.
- **tmsh::stop [args...]**
  Runs the command **stop** using the specified arguments.

The following Tcl commands provide structured access for retrieving configuration, statistics, and status information.

- **tmsh::get_config [args...]**
  Returns a list of Tcl objects. Each of these objects can be passed to the commands that accept an **$obj** argument. The arguments for this command are the same as for the **tmsh list** command.
- **tmsh::get_status [component] [args...]**
  Returns a list of Tcl objects that can be passed to the following commands that accept an **$obj** argument. The arguments to this command are the same as the **tmsh show** command.
  This command can only be used on components that accept the **field-fmt** option. The **field-fmt** option is automatically appended to the argument list. The **tmsh** help pages identify if a component supports the **field-fmt** option.
  That there are very few components that have status and statistics that do not support the **field-fmt** option, and in those cases you can use the Tcl **tmsh::show** command to retrieve the object in the form of a Tcl string object.
  A component must be specified, for example, **tmsh::get_status ltm pool**.
- **tmsh::get_type $obj**
  Returns the type identifier associated with the object. The **$obj** argument must be an object that was returned by either of the Tcl **tmsh::get_config** or **tmsh::get_status** commands.
- **tmsh::get_name $obj**
  Returns the object identifier associated with the object. The **$obj** argument must be an object that was returned by either of the Tcl commands **tmsh::get_config** or **tmsh::get_status**.
- **tmsh::get_field_names [value | nested] $obj**
  Returns a list of field names (not the value associated with a field) that are present in an object. The **value** fields are simple values or lists (for example, an integer or a string). The **nested** fields are a collection of zero or more nested objects, where the nested objects have their own fields (for example, pool members, and virtual server profiles).
  The **$obj** argument must be an object that was returned by the Tcl **tmsh::get_config** or **tmsh::get_status** commands. If the object was retrieved using the Tcl **tmsh::get_config** command, the field names are identical to those that are displayed by the **tmsh list** command. If the object was retrieved using the Tcl **tmsh::get_status** command, the fields are identical to those that the system displays using the **tmsh show** command with the **field-fmt** option.
- **tmsh::get_field_value $obj [field name] [Tcl variable]**
  Retrieves the value of **field name**.
  The **Tcl variable** is optional. The behavior of this command depends on whether **field name** is present in $obj and a **Tcl variable** is present in the command.
  - If **field name** is present in **$obj**, and a **Tcl variable** is present, the **Tcl variable** is set to the value of **field name** and the command returns **1**.

- If **field name** is not present in **$obj**, and a **Tcl variable** is present, the command returns **0** (zero).
- If **field name** is present in **$obj**, and a **Tcl variable** is not present, the command returns the field value.
- If **field name** is not present in **$obj**, and a **Tcl variable** is not present, the command raises an error that causes the script to stop. You can use the Tcl command **catch** to recognize the error and continue to run the script.

The **$obj** argument must be an object that was returned by the Tcl **tmsh::get_config** or **tmsh::get_status** commands, or a nested object obtained from the Tcl **tmsh::get_field_value** command.

If the field is a set of nested objects, the Tcl object that the system returns is a list of objects, where each of the objects can contain fields. Each of the objects can be passed to the Tcl **tmsh::get_field_value** command. If the field is not a nested object the system returns a single Tcl string object.

Transaction Control

The following Tcl commands are specific to the **tmsh** Tcl API. There are no corresponding commands available in **tmsh**.

- **tmsh::begin_transaction**
  Begins an update transaction. The Tcl **tmsh::create**, **tmsh::delete**, and **tmsh::modify** commands that are issued before the next Tcl **tmsh::commit_transaction** command are submitted as a single update. The system rolls back all of the commands if any of the commands fail.
- **tmsh::commit_transaction**
  Runs the commands that have been issued since the last Tcl **tmsh::begin_transaction** command. The system validates all of the commands against the running configuration. If any one of the commands fail, the system does not apply any of the commands to the running configuration.
- **tmsh::cancel_transaction**
  Cancels all commands that you have issued since the last Tcl **tmsh::begin_transaction** command.

Important

You cannot use these Tcl commands inside an active transaction:

- **tmsh::list**
- **tmsh::show**
- **tmsh::get_config**

- **tmsh::get_status**

Logging

You can use the following Tcl commands to generate log events. These commands affect the behavior of the script and do not affect **tmsh**. These commands are available only to users who have been assigned either the **Administrator** or **Resource Administrator** role.

- **tmsh::log_dest [screen | file]**
  Specifies whether the system sends events to the screen or to log files. If **file** is selected, log messages will be directed to **/var/log/ltm**.
- **tmsh::log_level [level]**
  Specifies the default severity level. The system does not log events below the specified level. The options, listed in decreasing order of severity, are:
  - **emerg**
  - **alert**
  - **crit**
  - **err**
  - **warning**
  - **notice**
  - **info**
  - **debug**
- **tmsh::log [level] "message..."**
  Logs the specified message. The level parameter is optional. The level can be one of those described in the Tcl **tmsh::log_level** command.

Custom Istats

Custom **counter**, **gauge**, and **string** fields may be created, modified, and retrieved using iRules or tmsh scripts. These custom fields are created on first write and do not need to be declared separately.

Each custom field has a "key" that can be associated with a tmsh configuration object. This key is composed of a **tmsh** component dotted path, a specific object name or ID, the field type, and the field name. The entire key must be enclosed in quotes.

For example, **"ltm.pool /Common/my_pool counter num_hits"** refers to the **num_hits** counter associated with the LTM pool named **my_pool**, located in the **Common** folder.

These custom fields are displayed with the **tmsh show** command on the associated object.

- **istats::incr [key] [amount]**
  Increments a custom counter by **amount**.
- **istats::set [key] [value]**
  Sets a custom gauge or string to **value**. Setting a counter to an exact value will only set it in the local segment, but **istats::get** will always read the aggregated (not local) value.
- **istats::get [key]**
  Returns the latest aggregated value of the custom field or **0** (zero) if it does not exist (**""** for string fields).
- **istats::remove [key]**
  Removes the custom field from all segments on all blades. Effectively resets a counter to 0.

Utilities

The following commands are TCL utility commands.

- **tmsh::clear_screen**
  Clears the screen and places the cursor at the upper left of the screen.
- **tmsh::display [variable | command output]**
  Provides access to the **tmsh** pager. Output generated with the Tcl **puts** command is not paged.
- **tmsh::display_threshold [integer]**
  When a script is run, the system disables the option **cli preference display-threshold**.
  You can use the Tcl **tmsh::display_threshold** command to re-enable the threshold. Re-enabling the threshold in this way causes the script to generate a prompt if you issue the **tmsh::list**, **tmsh::show**, **tmsh::get_config**, or **tmsh::get_status** commands, and the output that is generated exceeds the threshold. See **help cli preference** for a description of this option and valid ranges for its value.
- **tmsh::expand_macro [macro_text] options...**
  Expands a macro and returns the resulting string. A macro is a string containing macro syntax which can be used for parameter substitution, script and iRule templatization, etc. The Macro Syntax includes the following delimiters:
  <% The beginning of an expansion code block.
  <%= The beginning of an expansion code block. Spool the output after evaluating.
  <%D[0-9][0-9] The beginning of a debug/logging code block with the debug threshold set to 0 thru 99.
  <%D[0-9][0-9]= The beginning of a debug/logging code block with the debug threshold set to 0 thru 99. Spool the output after evaluating.

% > The end of the current block (works for all types).
Typically, the result of the **expand_macro** command is used as the input to another command (eg. ltm rule create). The command can be called multiple times within an iApp implementation to expand multiple macros.
macro_text is the blob of text to expand. If not specified, the command will expand the Macro section of the iApp. If no macro_text argument is specified and no Macro section exists for the iApp, an error will be issued.
-vars name_value_pair_list
Specifies a list of additional variables (name/value pairs) which can be referenced within the macro and expanded by the command. All APL variables are automatically available from within the macro, so the -vars option allows a way to specify additional variables from the iApp Implementaiton section. Since the variables are defined within a Tcl list the format is: { name1 value1 name2 ... nameN valueN }
-debug debug_levels
Specifies a single debug level or list of debug levels for controlling which debug messages get rendered in the expanded output.
-debuginclusive debug_level
Specifies a debug level for controlling which debug messages get rendered in the expanded output. Since it's "inclusive" all messages with a level at the specified level and below will get rendered in the expanded output.
The following example expands the macro defined in the Macro section of the iApp, and sets the debug level to render all debug messages with a level of 11, 33 or 66:
tmsh::expand_macro -debug {11 33 66}
The following example expands the macro defined via a Tcl variable (mac), adds two variables (foo and enable_mything), and sets the debug level to render all messages of level 66 and below:
tmsh::expand_macro $mac -vars {foo bar enable_mything true} -debuginclusive 66

- **tmsh::get_ifile_text [iFile name]**
  Retrieve the text contained in the specified text iFile. When used on an iFile containing characters which are non-ascii or are not printable/space, an error will be returned.
- **tmsh::include [script name]**
  Runs the Tcl **eval** command on the specified script. The system evaluates the script at a global level, and all procedures in the included script are available to any other procedure. You must have previously created the script that is being included using the **tmsh edit / cli script [name]** command. If a full path is not given for the script name, tmsh will attempt to first locate the script from the same folder as the including script, then the root partition folder of the including script, and finally the **/Common** folder.
- **tmsh::run_proc [script_name:proc_name] options...]**
  Runs the Tcl **eval** command on the specified script and process. The script **script_name** is loaded as if **tmsh::include** was called. After the script is loaded, the Tcl **eval** command is run on the specified Tcl

process. Any options that were specified are passed to the Tcl process. This is essentially a short form of running **tmsh::include script_name**, followed by running one of the Tcl processes contained in the script that was included.
The following example invokes the display_pool_status proc that is contained in the pool_utils script:
tmsh::run_proc pool_utils:display_pool_status

- **tmsh::stateless [disabled | enabled]**
  Modifies the behavior of **tmsh::create** and **tmsh::delete**.
  When stateless mode is **disabled**, an attempt to create an object that already exists in the configuration results in an error, and an attempt to delete an object that does not exist in the configuration is an error.
  When stateless mode is **enabled**, an attempt to create an object that already exists in the configuration does not result in an error, and an attempt to delete an object that does not exist in the configuration does not result in an error.
  Enabling stateless mode enables scripts to successfully run multiple times with the same input.
  The default value is **disabled**.
- **tmsh::version**
  Returns the version number of the BIG-IP system as a Tcl string. The version consists of three digits: a major, minor, and maintenance version, separated by periods. For example, **10.1.0** indicates minor version 1 of major version 10.

Context Sensitive Help

Use the following commands to create a script that provides context sensitive help when a user types **Tab** or question mark (**?**).

- **script::help**
  Scripts can provide the **script::help** procedure. **tmsh** invokes the procedure when a user types a question mark (**?**) while entering the command sequence **run / cli script [name]**. If the specified script includes the **script::init** procedure, **tmsh** invokes it before the **script::help** procedure. The script can add context sensitive help by calling the **tmsh::add_help** and **tmsh::builtin_help** procedures. **tmsh** formats the help and displays it.
- **script::tabc**
  Scripts can provide the **script::tabc** procedure. The system invokes this procedure when the user types **Tab** while entering the command sequence **run / cli script**. If the **script::init** procedure is included in the script, that procedure is invoked before the **script::tabc** procedure. The script can add tab completion datasets to the script by calling the **tmsh::add_tabc** and **tmsh::builtin_tabc** procedures. **tmsh** either formats and displays the tab completion datasets, or if possible, completes the current argument.

- **tmsh::csh**
  tmsh::csh is a Tcl string variable that can be used in the **script::init** procedure to determine the context in which the **script::init** procedure was invoked.
  tmsh::csh is set to one of the following:
  - **question mark (?)**
    Indicates that the user typed a question mark (**?**).
  - **TABC**
    Indicates the user pressed the **Tab** key.
  - **an empty string ""**
    Indicates the script is being run.
- **tmsh::add_help [[category item description] | [description]]**
  Displays context sensitive help when the user types a question mark (**?**). If you supply one argument, that argument displays as-is with no formatting applied to the description.
  If you supply three arguments, one or more datasets are constructed. The first argument is the name of the dataset. The second argument is an item in the dataset. The third argument is a description of the item. This command has an effect only if the Tcl **tmsh::csh** variable is set to question mark (**?**).
- **tmsh::builtin_help ["tmsh command" args...]**
  Presents the same results as typing a question mark (**?**) while entering a **tmsh** command. The system stores a set of possible completions and displays the possibilities when the **script::help** procedure returns. This command has an effect only if the Tcl **tmsh::csh** variable is set to question mark (**?**).
- **tmsh::add_tabc [[category item] | [item]]**
  Adds tab completion datasets. If you supply one argument, the system adds that argument to an anonymous dataset. If you supply two arguments, the system constructs one or more datasets. The first argument is the name of the dataset. The second argument is an item in the dataset. Potential completions are displayed in groups based on category. This command has an effect only if the Tcl **$tmsh::csh** variable is set to **TABC**.
- **tmsh::builtin_tabc ["tmsh command" args...]**
  Many of the **tmsh** commands that are available for scripting are also available in the interactive shell. A script can use the **tmsh::builtin_tabc** command to present the same tab completion results as a built-in command. The command does not return a value. The set of possible completions are stored internally and displayed when the **script::tabc** procedure returns. This command has an effect only if the Tcl **$tmsh::csh** variable is set to **TABC**.

Third Party Tcl Library Usage

A selection of third party libraries have been tested to work within the CLI script environment, including MD5, BASE64, SHA1/SHA256, HTTP, TLS, TCL Perl, LDAP client, and XML parser. The TCL packages can only reside in the directory of **/usr/share/tcl8.4**.

Important

Only these tested packages are supported currently.

This example demonstrates the use of a Tcl package command to make use of tls/https. The TLS package is installed in the directory **/usr/share/tcl8.4/tls** in the form of two files: tls.tcl and libtls1.6.1.so.

```
Modify script /Common/use_tls {

proc script::run {} {
    set pkg_name tls
    set pkg_version 1.6
    package require http
    if {[catch {package require $pkg_name pkg_version}]} {
        puts "No package found: $pkg_name!
    } else {
        puts "Found package: $pkg_name!
        http::register https 443 tls::socket
        set token [http::geturl https://172.27.42.161/]
        upvar #0 $token state
        puts $state(http)
        puts $state(body)
    }
  }
}
```

This example uses the callback function to handle http data.

```
cli script /Common/use_http2 {
proc script::httpCallback {token} {
        upvar #0 $token state
        puts $state(http)
        puts $state(body)
        incr ::got_something
}
proc script::run {} {
    namespace eval :: {
        set got_something 0
    }
    set pkg_name http
    set pkg_version 2.4.5
    if {[catch {package require $pkg_name $pkg_version}]} {
        puts "No package found: $pkg_name!
    } else {
        puts "Found package: $pkg_name!
        http::geturl http://172.27.42.22/index.htm -command script::httpCallback
        vwait ::got_something
    }
  }
}
```

This example uses the LDAP client package to query data.

```
cli script /Common/use_ldap {
proc script::run {} {
    set pkg_name ldap
    if {[catch {package require $pkg_name 1.8}]} {
        puts "No package found: $pkg_name!
    } else {
        puts "Found package: $pkg_name!
        set handle [ldap::connect 172.27.1.2]
        ldap::bind $handle
        set results [ldap::search $handle "dc=f5,dc=com" "(uid=test)" {}]
        foreach result $results {
            puts $result
        }
        ldap::unbind $handle
        ldap::disconnect $handle
    }
  }
}
```

Here are some additional examples:

```
cli script /Common/use_parray {
proc script::run {} {
        puts [info patch]
        namespace eval :: {
            set pkg_location /usr/share/tcl8.4/
            source [file join $pkg_location package.tcl]
        }
        puts "NS: [namespace current]"
        set pkg_location $::pkg_location
        source [file join $pkg_location parray.tcl]
        parray ::tcl_platform
  }
}
```

```
cli script /Common/use_sha2 {
proc script::run {} {
        set pkg_name sha256
        if {[catch {package require $pkg_name}]} {
            puts "No package found: $pkg_name!
        } else {
            puts "Found package: $pkg_name!
            puts "TCL does SHA2 now:"
            puts [sha2::sha256 "TCL does SHA2"]
        }
  }
}
```

```
cli script /Common/use_tclperl {
proc script::run {} {
        set pkg_name tclperl
        if {[catch {package require $pkg_name}]} {
            puts "No package found: $pkg_name!
        } else {
            puts "Found package: $pkg_name!
            set interpreter [perl::interp new]
            $interpreter eval {print "Hello World
            perl::interp delete $interpreter
       }
  }
}
```

Special Characters

There are several characters that are part of both Tcl and **tmsh** syntax. You must escape these characters in a shell script so that Tcl passes them to **tmsh**. You can use standard Tcl escape characters, such as quotes and back slashes. You must escape curly braces ({ }), for example, "{" "}".

- **tmsh::create ltm pool my_pool members add "{ 10.1.2.3:80 }"**
  Creates a Local Traffic Manager pool named **my_pool**.

Disabled Commands

The following commands are disabled for users that have not been assigned a user role of **Administrator** or **Resource Administrator**:

- auto_execok
- auto_import
- auto_load
- auto_mkindex
- auto_mkindex_old
- auto_qualify
- auto_reset
- bgerror
- cd
- close
- eof
- exec
- fblocked
- fconfigure
- fcopy
- file

- filevent
- filename
- flush
- glob
- http
- interp
- load
- memory
- open
- package
- pid
- pkg:create
- pkg_mkindex
- pwd
- seek
- socket
- source
- tcl_findLibrary
- tell
- unknown
- updates
- vwait

Examples

The following example demonstrates the use of all **tmsh** Tcl commands. The script displays all configuration property values or all status and statistic values for the specified component, depending on the specified arguments. The system displays all configuration settings if you replace **[tmsh::get_config $comp all-properties]** with **[tmsh::get_config / all-properties]**. The use of the **all-properties** option ensures that all options are displayed.

This command sequence is an example of how to run the following script: **run / cli script example.tcl config ltm pool**.

```
cli script example.tcl {

proc script::init { } {
    set ::field_fmt "%-25s %s"
    set ::usage_string "usage: [lindex $tmsh::argv 0] \
        <config | status> <component path... name>"
}

proc script::help { } {
    if { $tmsh::argc < 2 } {
        tmsh::add_help Options: config "Display configuration"
        tmsh::add_help Options: status \
  "Display status and statistics"
    }
    else {
        build_csh tmsh::builtin_help
    }
}

proc script::tabc { } {
    if { $tmsh::argc < 2 } {
        tmsh::add_tabc config
        tmsh::add_tabc status
    }
    else {
        build_csh tmsh::builtin_tabc
    }
}

proc script::run { } {
    if { $tmsh::argc < 3 } {
        usage
    }
    set opt [lindex $tmsh::argv 1]
    if { $opt != "config" && $opt != "status" } {
        usage
    }
    set comp ""
    for {set idx 2} {$idx < $tmsh::argc} {incr idx} {
        append comp "[lindex $tmsh::argv $idx] "
    }

if { $opt == "config" } {
    set objs [tmsh::get_config $comp all-properties]
}
else {
    set objs [tmsh::get_status $comp]
}

set idx 0
set total [llength $objs]
```

```
while { $idx < $total } {
    set obj [lindex $objs $idx]
    print_object obj
    puts ""
    incr idx;
}
      }
proc print_fields { objVar } {
    upvar $objVar obj
    set fdx 0
    set fields [tmsh::get_field_names value $obj]
    set field_count [llength $fields]
    while { $fdx < $field_count } {
        set field [lindex $fields $fdx]
        puts [format $::field_fmt $field \
            [tmsh::get_field_value $obj $field]]
        incr fdx
    }
}
proc print_object { objVar } {
    upvar $objVar obj
    puts "[tmsh::get_type $obj] [tmsh::get_name $obj]"
# name/value pairs
print_fields obj
# nested objects
set fdx 0
set fields [tmsh::get_field_names nested $obj]
set count [llength $fields]
while { $fdx < $count } {
    set field [lindex $fields $fdx]
    set nested_objects [tmsh::get_field_value $obj $field]
    set ndx 0
    set n_count [llength $nested_objects]
    while { $ndx < $n_count } {
        set nobj [lindex $nested_objects $ndx]
        print_object nobj
        incr ndx
    }
    if {$n_count == 0 } {
        puts [format $::field_fmt $field "none"]
    }
    incr fdx
}
      }
proc build_csh { command } {
    # generate context sensitive help, tab completion or "?"
    set args ""
    for {set idx 2} {$idx < $tmsh::argc} {incr idx} {
        lappend args [lindex $tmsh::argv $idx]
    }
    set opt [lindex $tmsh::argv 1]
    if { $opt == "config" } {
        $command list $args
    }
    elseif { $opt == "status" } {
        $command show $args
    }
    else {
        puts "
```

```
    }
    return $args
}
proc usage { } {
    puts $::usage_string
    exit
}
  }
```

Examples

The following example demonstrates the scripts using 11.6.0 tmsh syntax.

```
cli script example_ver.tcl {
   ...
   proc script::run {} {
       tmsh::modify cli version active 11.6.0
       # the tmsh command in the section below should contain 11.6.0 tmsh syntax
       puts stdout [tmsh::list ltm pool mypool]
       ...
  }
}
```

The following example demonstrates the scripts that are using multiple tmsh syntaxes.

```
cli script example_multi_ver.tcl {
   ....
   proc script::run {} {
       tmsh::modify cli version active 11.5.0
       # the tmsh command in the section below should contain 11.5.0 tmsh syntax
       puts stdout [tmsh::list ltm pool mypool]
       ...
tmsh::modify cli version active 11.6.0
# the tmsh command in the section below should contain 11.6.0 tmsh syntax
puts stdout [tmsh::list ltm pool mypool]
...
   }
 }
```

See Also

cli alias, *create*, *delete*, *edit*, glob, *list*, *modify*, regex, *reset-stats*, *show*, *tmsh* and *generate*.

For information about Tcl, see www.tcl.tk.

transaction

Opens batch mode within which you can submit a set of commands as a single transaction.

Syntax

Use the **transaction** component within the **cli** module to open batch mode, enter a series of commands, and then submit the commands as a single transaction.

Create/Modify

```
create transaction
modify transaction
    delete [entry_id]
submit transaction
```

Display

```
list transaction
```

Delete

```
delete transaction
```

Description

tmsh parses each command that you enter in batch mode. If the command passes a syntax check, **tmsh** saves it as part of the transaction you are creating and returns a confirmation. After you finish adding commands, you submit the transaction to change the running configuration of the system. You must run the **save config** command to save the changes to the stored configuration files.

If, while creating a transaction, you decide you do not want to change the running configuration, you can delete the transaction rather than submit it. However, you can recreate a transaction that you have deleted by using the **cli history** component.

There are a few commands that you can enter on the command line that the system immediately runs, rather than adding the commands to a transaction. These commands are **list** and **show**. Additionally, **tmsh** immediately runs the command sequence **run bigpipe**, but does not add it to the transaction.

Examples

The following example shows the commands that you enter from within the **ltm** module to create and submit a transaction that creates a Local Traffic Manager pool and virtual server, and then associates the two.

1. Open **tmsh** batch mode:
   create /cli transaction
2. Add a command to the transaction that creates **pool1** for the Local Traffic Manager using the default values for a pool:
   create pool pool1
3. Add a command to the transaction that creates the virtual server **virtual1** for the Local Traffic Manager using the default values for a virtual server, and associates it with **pool1**.
   create virtual virtual1 pool pool1
4. Display, in a numbered list, the current set of commands in the transaction:
   list /cli transaction

◆ Note

You can use the preceding command to determine the entry ID of a command. Then, you can use this ID to remove or replace a command in the transaction, or to identify a command before which you want to insert another command.

5. Submit the transaction:
   submit /cli transaction

Options

- **command**
  Specifies, in quotation marks, the full path to a command to add to or delete from the transaction that you are creating. You can also replace an existing command with another command or insert a command before a command in the transaction.
- **create**
  Opens batch mode.
- **delete**
  Deletes the transaction that you are creating and closes batch mode.
- **list**
  Displays, in a numbered list, the current set of commands in the transaction that you are creating.
- **modify**
  Specifies a previously entered line in the transaction that you want to change. The options are:

- **delete**
  Deletes the specified entries from the transaction that you are creating.
- **entry_id**
  Specifies the number of a command in the list of commands in the transaction that you want to delete.

◆ **submit**
Submits the transaction that you are entering and closes batch mode. The transaction is submitted in the context of the **cli admin-partitions** settings that are active when the **submit** command is issued.

See Also

admin-partitions, *create*, *delete*, *list*, *modify*, *submit*, *tmsh*

version

Displays and Configures **tmsh** versions.

Syntax

Configure the **version** component within the **cli** module using the syntax shown in the following sections.

Modify

```
modify version [option]
    active [string ]
```

Display

```
show version
```

Description

You can use the **version** component to configure **tmsh** to run the specified version.

Examples

modify cli version active 11.5.0

Configures **tmsh** run 11.5.0 version.

show cli version

Displays the latest, active and supported versions of TMSH.

Options

- **active**
  Specifies the active version of TMSH.
- **latest**
  Displays TMSH the latest version. This is used as the default version.
- **supported**
  Displays the current supported TMSH versions on the system.
- **imported**
  Displays the imported TMSH versions on the system. An imported TMSH version will be imported from a UCS created from TMSH version which is not supported in the current system - a very rare case. Be aware, for an imported TMSH version, only syntax is supported, if it requires

other handling other than syntax change, it will not supported. So, for an imported TMSH version, it is not fully supported. By default, this entry will not be displayed unless preference is set.

See Also

show, *modify*, *ucs*, *tmsh*

44

cli alias

- Introducing the cli alias module
- Alphabetical list of components

Introducing the cli alias module

You can use the tmsh components that reside within the cli alias module to configure administrative partitions, aliases, and the command line preferences. For more information about the tmsh hierarchical structure, see Chapter 2, *Understanding and Using the Traffic Management Shell*.

Alphabetical list of components

The remainder of this chapter lists the tmsh components that are available in the cli alias module.

private

Configures a user private alias.

Syntax

Configure the **alias** component within the **cli alias** module using the syntax in the following sections.

Create/Modify

```
create private [name]
    command [commandSyntax]
    command ["command syntax"]
    command "[command syntax]; [command syntax]; ..."
    app-service [[string] | none]
    description [string]
edit private [name]
    all
modify alias [name]
    command [commandSyntax]
    command ["command syntax"]
    command "[command syntax]; [command syntax]; ..."
```

Display

```
list private
list alias [ [ [name] | [glob] | [regex] ] ...]
show running-config private
show running-config private [ [ [name] | [glob] | [regex] ] ...]
    all-properties
    one-line
    non-default-properties
```

Delete

```
delete private [all | [name ... name] ]
```

Description

You can use the **private** component to create a shortcut that runs a **tmsh** command sequence. The name of the private alias is what you type on the command line to run the command. If the command sequence for which you are creating an alias contains spaces, it must be enclosed in quotation marks. Command aliases are not case-sensitive.

You can create a private alias that runs multiple commands by entering the command sequences separated by semi-colons.

Private aliases can be used only by the user who created them.

When a batch mode transaction is active, commands that operate on the **private** component are run immediately and are not added to the transaction.

Examples

create private save command "save config"

Creates an alias that saves the running configuration in the stored configuration files from anywhere within **tmsh**.

create private stats command "show /sys traffic"

Creates an alias that displays traffic statistics from anywhere within **tmsh**.

create private nodemonitor command "list /ltm node; list /ltm monitor"

Creates an alias that displays the Local Traffic Manager nodes and monitors.

create private myalias command "show /sys provision ; show /sys license"

Creates an alias that displays license and provisioning information.

create private ltmpool command "list /ltm pool"

Creates an alias that displays the Local Traffic Manager pools from anywhere within **tmsh**.

Options

- **command syntax**
  Specifies the command for which you are creating an alias. To create an alias that runs multiple commands, enter the command sequences separated by semi-colons.
- **app-service**
  Specifies the name of the application service to which the alias belongs. The default value is **none**. **Note:** If the **strict-updates** option is **enabled** on the application service that owns the object, you cannot modify or delete the alias. Only the application service can modify or delete the alias.
- **description**
  Specifies the purpose of the alias. If you enable **cli preference show-aliases**, **tmsh** displays the description in context-sensitive help (**?**).
- **glob**
  Displays the items that match the **glob** expression. See **help glob** for a description of **glob** expression syntax.
- **name**
  Specifies a name for the alias. This is what you type in **tmsh** to run the command for which you are creating an alias.

- **regex**
  Displays the items that match the regular expression. The regular expression must be preceded by an at sign (@[regular expression]) to indicate that the identifier is a regular expression. See **help regex** for a description of regular expression syntax.

See Also

create, *delete*, *edit*, glob, *list*, *modify*, regex, *show*, *shared*, *tmsh*

shared

Configures a shared alias.

Syntax

Configure the shared **alias** component within the **cli alias** module using the syntax in the following sections.

Create/Modify

```
create shared [name]
    command [commandSyntax]
    command ["command syntax"]
    command "[command syntax]; [command syntax]; ..."
    app-service [[string] | none]
    description [string]
edit shared [name]
    all
modify alias [name]
    command [commandSyntax]
    command ["command syntax"]
    command "[command syntax]; [command syntax]; ..."
```

Display

```
list shared
list alias [ [ [name] | [glob] | [regex] ] ...]
show running-config shared
show running-config shared [ [ [name] | [glob] | [regex] ] ...]
    all-properties
    one-line
    non-default-properties
```

Delete

```
delete shared [all | [name ... name] ]
```

Description

You can use the **shared** component to create a shortcut to run a **tmsh** command sequence. The name of the shared alias is what you type on the command line to run the command. If the command sequence for which you are creating an alias contains spaces, it must be enclosed in quotation marks. Command aliases are not case-sensitive.

You can create a shared alias that runs multiple commands by entering the command sequences separated by semi-colons.

Shared aliases can be used by all users.

When a batch mode transaction is active, commands that operate on the **shared** component are run immediately and are not added to the transaction.

Examples

create shared save command "save config"

Creates an alias that saves the running configuration in the stored configuration files from anywhere within **tmsh**.

create shared stats command "show /sys traffic"

Creates an alias that displays traffic statistics from anywhere within **tmsh**.

create shared nodemonitor command "list /ltm node; list /ltm monitor"

Creates an alias that displays the Local Traffic Manager nodes and monitors.

create shared myalias command "show /sys provision ; show /sys license"

Creates an alias that displays license and provisioning information.

create shared ltmpool command "list /ltm pool"

Creates an alias that displays the Local Traffic Manager pools from anywhere within **tmsh**.

Options

- **command syntax**
  Specifies the command for which you are creating an alias. To create an alias that runs multiple commands, enter the command sequences separated by semi-colons.
- **app-service**
  Specifies the name of the application service to which the alias belongs. The default value is **none**. **Note:** If the **strict-updates** option is **enabled** on the application service that owns the object, you cannot modify or delete the alias. Only the application service can modify or delete the alias.
- **description**
  Specifies the purpose of the alias. If you enable **cli preference show-aliase**, **tmsh** displays the description in context-sensitive help (**?**).
- **glob**
  Displays the items that match the **glob** expression. See **help glob** for a description of **glob** expression syntax.
- **name**
  Specifies a name for the alias. This is what you type in **tmsh** to run the command for which you are creating an alias.
- **regex**
  Displays the items that match the regular expression. The regular expression must be preceded by an at sign (@[regular expression]) to indicate that the identifier is a regular expression. See **help regex** for a description of regular expression syntax.

See Also

create, *delete*, *edit*, glob, *list*, *modify*, regex, *show*, *shared*, *tmsh*

45

cm

- Introducing the cm module
- Alphabetical list of components

Introducing the cm module

You can use the tmsh components that reside within the cm module to manage devices, device groups, and trust relationships. For more information about the tmsh hierarchical structure, see Chapter 2, *Understanding and Using the Traffic Management Shell*.

Alphabetical list of components

The remainder of this chapter lists the tmsh components that are available in the cm module.

cert

Manages a CM trust certificate file.

Syntax

Display or delete the **cert** component within the **cm** module using the syntax shown in the following sections.

Display

```
list cert
list cert [ [ [name] | [glob] | [regex] ] ... ]
show running-config cert
show running-config cert [ [ [name] | [glob] | [regex] ] ... ]
    all-properties
    app-service
    certificate-key-size
    checksum
    create-time
    created-by
    email
    expiration-date
    expiration-string
    fingerprint
    is-bundle
    issuer
    key-type
    last-update-time
    mode
    non-default-properties
    one-line
    partition
    recursive
    revision
    serial-number
    size
    source-path
    subject
    subject-alternative-name
    system-path
    updated-by
    version
```

Delete

```
delete cert [name]
```

Description

You can use the **cert** component to display or delete a CM trust certificates.

Options

- **app-service**
  Displays the application service to which the object belongs. The default value is **none**. **Note:** If the **strict-updates** option is **enabled** on the Application Service that owns the object, you cannot modify or delete the object. Only the Application Service can modify or delete the object.
- **certificate-key-size**
  Displays the number of bits in the key associated with this certificate.
- **checksum**
  Displays a cryptographic hash or checksum of the file contents for use in verification of file integrity.
- **create-time**
  Displays the time at which the trust certificate was created.
- **created-by**
  Displays the name of the person, who originally created the trust certificate.
- **email**
  Displays the email of the person, who originally created the trust certificate.
- **expiration-date**
  Displays the date at which the trust certificate expires. The date is stored as a POSIX time.
- **expiration-string**
  Displays a string representation of the trust certificate expiration date.
- **fingerprint**
  Specifies the cryptographic fingerprint of the trust certificate.
- **glob**
  Displays the items that match the glob expression. See **help glob** for a description of **glob** expression syntax.
- **is-bundle**
  Indicates whether the trust certificate file is a bundle (that is, whether it contains more than one certificate).
- **issuer**
  Displays the X.509 information for the issuer of the trust certificate. If the trust certificate is a bundle, then this displays the issuer information for the primary (first) trust certificate in the bundle.
- **key-type**
  Displays the type of cryptographic key associated with this trust certificate.
- **last-update-time**
  Displays the last time the trust certificate was modified.
- **mode**
  Displays the UNIX® file permissions mode for the file associated with this trust certificate as a numerical value.
- **partition**
  Displays the partition within which the trust certificate file resides.

- **recursive**
  Displays all objects of the specified type and the folder that contains the object.
- **regex**
  Displays the items that match the regular expression. The regular expression must be preceded by an at sign (@[regular expression]) to indicate that the identifier is a regular expression. See **help regex** for a description of regular expression syntax.
- **revision**
  Displays the number of the latest revision of the trust certificate. The revision starts with 1 and increments on each update.
- **serial-number**
  Displays the serial number of the trust certificate.
- **size**
  Displays the size (in bytes) of the file associated with the trust certificate.
- **source-path** [URL]
  Displays the path to the source of the trust certificate as a URL, for example:

source-path http://cert-server/cert_store/certs/vs_132.key

source-path https://cert-server/cert_store/certs/vs_132.key

source-path ftp://username:password@server/cert_store/certs/vs_132.key

- **subject**
  Displays X.509 information about the subject of the trust certificate. If the certificate is a bundle, then the subject information for the primary (first) trust certificate in the bundle displays.
- **subject-alternative-name**
  Displays a standard X.509 extension as shown in RFC 2459.
- **system-path**
  Displays the path to the trust certificate.
- **updated-by**
  Displays the name of the person, who last updated the trust certificate.
- **version**
  Displays the X.509 version of the trust certificate.

See Also

delete, glob, *list*, regex, *tmsh*

config-sync

Manually synchronizes the configuration between devices.

Syntax

Run the **config-sync** program within the **cm** module using the syntax in the following section.

Modify

```
run config-sync
    from-group <name>
    recover-sync
    to-group <name>
```

Description

You must use only one of the options when you run configuration synchronization. The three options are mutually exclusive.

Examples

run config-sync from-group /Common/my_dg

Updates the configurations on the remote devices in the device group **Common/my_dg** with the configuration on the local device. If the local device does not have the newest configuration, then the configuration synchronization does nothing.

run config-sync to-group /Common/my_dg

Updates the configuration on the local device with the configuration from the remote device in the device group **Common/my_dg** with the newest configuration. If the local device already has the newest configuration, then the configuration synchronization does nothing.

run config-sync recover-sync

Resets the local device configuration and restores the trust domain, device, and device-group information to default settings.

Options

- **from-group**
  Updates the configuration of the local device with the configuration of the remote device in the specified device group that has the newest configuration. If the local device already has the newest configuration, then the configuration synchronization does nothing. This option is mutually exclusive of the **to-group** and **recover-sync** options.

- **recover-sync**
  Resets the local device configuration and restores the trust domain, device, and device-group information to default settings. After this recovery, you can sync the local device with its peers by running **config-sync** on a peer device and specifying the device group in which the local device is a member. This option is mutually exclusive of the **from-group** and **to-group** options.
- **to-group**
  Updates the configurations of the remote devices in the specified device group with the configuration of the local device. If the local device does not have the newest configuration, then the configuration synchronization does nothing. This option is mutually exclusive of the **from-group** and **recover-sync** options.

See Also

run, *tmsh*

device

Manages a device.

Syntax

Manage the **device** component within the **cm** module using the syntax shown in the following sections.

Create/Modify

```
create device [name]
modify device [name]
   comment [string]
   configsync-ip [ip address | none]
   contact [string]
   description [string]
   ha-capacity [integer]
   hostname [string]
   location [string]
   mirror-ip [ip address | any6]
   mirror-secondary-ip [ip address | any6]
   multicast-interface [string]
   multicast-ip [ip address]
   multicast-port [integer]
   unicast-address [add | delete | modify | replace-all-with] {
       [unicast address]
   }
edit device [ [ [name] | [glob] | [regex] ] ... ]
    all-properties
    non-default-properties
```

Display

```
list device
list device [ [ [name] | [glob] | [regex] ] ... ]
show running-config device
show running-config device [ [ [name] | [glob] | [regex] ] ... ]
  active-modules
  all-properties
  app-service
  base-mac
  build
  cert
  chassis-id
  chassis-type
  failover-stats
  inactive-modules
  key
  location
  management-ip
  marketing-name
  non-default-properties
  one-line
  optional-modules
  partition
```

```
  platform-id
  product
  recursive
  self-device
  time-limited-modules
  time-zone
  version
show device-group
show device-group [name]
  all
  field-fmt
```

Delete

```
delete device [name]
```

Description

You can use the **device** component to manage devices.

WARNING

F5 Networks recommends that you do not create or delete devices. Instead, to add or remove devices on the BIG-IP system, modify the Root trust domain. For more information, see ***help trust-domain****.*

Options

- **active-modules**
  Displays the licensed modules that are currently active on the device.
- **app-service**
  Displays the application service to which the object belongs. The default value is **none**. **Note:** If the **strict-updates** option is **enabled** on the Application Service that owns the object, you cannot modify or delete the object. Only the Application Service can modify or delete the object.
- **base-mac**
  Displays the base MAC address for the device.
- **build**
  Displays the software build number.
- **cert**
  Displays the identity certificate used for device trust.
- **chassis-id**
  Displays the chassis identifier.
- **chassis-type**
  Displays the chassis type. The possible values are **individual** and **viprion**.
- **comment**
  Specifies user comments about the device.

- **configsync-ip**
  Specifies the IP address used for configuration synchronization. If you specify a self IP address, the self IP address object must be located in the Common folder.
- **contact**
  Specifies administrator contact information.
- **description**
  Specifies a user-defined description of the device.
- **edition**
  Displays the software edition.
- **failover-state**
  Displays the device failover state.
- **glob**
  Displays the items that match the glob expression. See **help glob** for a description of **glob** expression syntax.
- **ha-capacity**
  Specifies a number that represents the relative capacity of the device to be active for a number of traffic groups. This value along with the traffic group's ha-load-factor is used by the failover daemon to make traffic groups active amongst the available devices. The value is zero by default which means the device may run any number of traffic groups. The value must be within a valid range: **0** - **100000** inclusive.
- **hostname**
  Specifies a hostname for the device.
- **inactive-modules**
  Displays the licensed modules that are currently inactive on the device.
- **key**
  Displays the identity key used for device trust.
- **location**
  Specifies the physical location of the device.
- **marketing-name**
  Displays the marketing name of the device platform.
- **mirror-ip**
  Specifies the IP address used for state mirroring. If you specify a self IP address, the self IP address object must be located in the Common folder.
- **mirror-secondary-ip**
  Specifies the secondary IP address used for state mirroring. If you specify a self IP address, the self IP address object must be located in the Common folder.
- **multicast-interface**
  Specifies the interface name used for the failover multicast IP address.
- **multicast-ip**
  Specifies the multicast IP address used for failover.
- **multicast-port**
  Specifies the multicast port used for failover.

- **optional-modules**
  Displays the modules that are available for the current platform, but are not currently licensed.
- **platform-id**
  Displays the device platform identifier.
- **product**
  Displays the software product name.
- **recursive**
  Displays all objects of the specified type and the folder that contains the object.
- **regex**
  Displays the items that match the regular expression. The regular expression must be preceded by an at sign (@[regular expression]) to indicate that the identifier is a regular expression. See **help regex** for a description of regular expression syntax.
- **self-device**
  Displays **true**, when the device is the self device.
- **time-limited-modules**
  Displays the licensed modules that are time-limited.
- **time-zone**
  Displays the time zone configured on the device.
- **unicast-address**
  Displays the set of unicast IP addresses used for failover. If you specify a self IP address, the self IP address object must be located in the Common folder.
- **version**
  Displays the software version number.

See Also

create, *delete*, *edit*, glob, *list*, *modify*, regex, *show*, *tmsh*, *trust-domain*

device-group

Configures device groups.

Syntax

Modify the **device-group** component within the **cm** module using the syntax shown in the following sections.

Create/Modify

```
create device-group [name]
modify device-group [name]
  app-service [[string] | none]
  asm-sync [ enabled | disabled ]
  auto-sync [ enabled | disabled ]
  description [string]
  devices [add | delete | modify | replace-all-with] {
      [ device_name ]
  }
  full-load-on-sync [true | false]
  incremental-config-sync-size-max [integer]
  network-failover [ enabled | disabled ]
  save-on-auto-sync [true | false]
  type [ sync-only | sync-failover ]
  clear-incremental-config-sync-cache
edit device-group [ [ [name] | [glob] | [regex] ] ... ]
    all-properties
    non-default-properties
```

Display

```
list device-group
list device-group [ [ [name] | [glob] | [regex] ] ... ]
show running-config device-group
show running-config device-group [ [ [name] | [glob] | [regex] ] ... ]
  all-properties
  app-service
  non-default-properties
  partition
  recursive
show device-group
show device-group [name]
   field-fmt
```

Delete

```
delete device-group [name]
```

◆ Note

The device group must be empty, and you must remove all references to the device group, before you can delete the device group.

Description

You can use the **device-group** component to manage sets of devices used for configuration synchronization and failover.

Examples

create device-group my_device_group devices add {
/Common/device1
/Common/device2
}

Creates a sync-only device group named **my_device_group** with two devices, **device1** and **device2**.

delete device-group my_device_group

Deletes the device group named **my_device_group**.

list device-group my_device_group

Displays properties of the device group named **my_device_group**.

modify device-group my_device_group clear-incremental-config-sync-cache

WARNING

Do not use this option without assistance from the F5 Technical Support team.

Clears the incremental configuration synchronization cache. The next configuration synchronization for **my_device_group** that pulls configuration from this device will be a full load.

Options

- **app-service**
  Specifies the application service to which the object belongs. The default value is **none**. **Note:** If the **strict-updates** option is **enabled** on the Application Service that owns the object, you cannot modify or delete the object. Only the Application Service can modify or delete the object.
- **asm-sync**
  Specifies whether to synchronize ASM configurations of device group members. The default value is **disabled**. A device can be a member of only one ASM-enabled device group.
- **auto-sync**
  Specifies whether the device group automatically synchronizes configuration data to its members. The default value is **disabled**. Configuration will be saved on remote devices after receiving configuration updates if **save-on-auto-sync** is enabled.

- **clear-incremental-config-sync-cache**

WARNING

Do not use this option without assistance from the F5 Technical Support team.
The incremental configuration synchronization mechanism keeps a cache of transactions in each device group. Specifying this option will remove all transactions from the cache for the given device groups. This will not remove configuration from the device group, but will cause the next load in that group from the current device to be a full load.

- **description**
  Specifies a user-defined description of the device group.
- **devices**
  Adds, deletes, or replaces a set of devices to a device group by specifying the device name(s). When the local device is removed from a device group then all of the **sys folder** s that are associated with the device group are reset to have no device group and the name of each folder that was updated is logged to /var/log/ltm.
- **full-load-on-sync**
  Specifies that the entire configuration for a device group is sent when configuration synchronization is performed. The default value is **false**.
- **glob**
  Displays the items that match the glob expression. See **help glob** for a description of **glob** expression syntax.
- **incremental-config-sync-size-max**
  Specifies the maximum size (in KB) to devote to incremental config sync cached transactions. The default is 1024 KB."
- **name**
  Specifies a unique name for the component. This option is required for the commands **create**, **delete**, and **modify**.
- **network-failover**
  When the device group **type** is **failover**, specifies whether network failover is used.
- **partition**
  Displays the administrative partition within which the device group resides.
- **recursive**
  Displays all objects of the specified type and the folder that contains the object.
- **regex**
  Displays the items that match the regular expression. The regular expression must be preceded by an at sign (@[regular expression]) to indicate that the identifier is a regular expression. See **help regex** for a description of regular expression syntax.

- **save-on-auto-sync**
  Specifies whether to save the configuration on the remote devices following an automatic configuration synchronization. A device group configured for manual synchronization will always save on the remote devices regardless of this setting.
- **type**
  Specifies the type of device group. You can use this option only when you create a device group. You cannot modify the type of a device group. The default value is **sync-only**.

See Also

create, *delete*, *device*, *edit*, glob, *list*, *modify*, regex, *tmsh*

failover-status

Display the failover status of the local device.

Syntax

Display **failover-status** component within the **cm** module using the syntax in the following section.

Display

```
show failover-status
    field-fmt
```

Description

You can use the **failover-status** component to display the failover status of the local device.

For information about the options that you can use with the command **show**, see **help show**.

Example

show failover-status

Displays the failover status of the local device.

See Also

show, *tmsh*

key

Manages a CM trust certificate private key file.

Syntax

Display or delete a **key** component within the **cm** module using the syntax shown in the following sections.

Display

```
list key
list key [ [ [name] | [glob] | [regex] ] ... ]
show running-config key
show running-config key [ [ [name] | [glob] | [regex] ] ... ]
  all-properties
  app-service
  checksum
  create-time
  created-by
  key-size
  key-type
  last-update-time
  mode
  non-default-properties
  one-line
  partition
  recursive
  revision
  security-type
  size
  source-path
  system-path
  updated-by
```

Display

```
delete key [name]
```

```
=head1 DESCRIPTION
```

You can use the following options with the **key** component.

Options

- **app-service**
  Displays the application service to which the object belongs. The default value is **none**. **Note:** If the **strict-updates** option is **enabled** on the Application Service that owns the object, you cannot modify or delete the object. Only the Application Service can modify or delete the object.
- **checksum**
  Displays a cryptographic hash or checksum of the key for use in verification of key integrity.

- **create-time**
  Displays the time at which the key was created.
- **created-by**
  Displays the user who originally created the key.
- **glob**
  Displays the items that match the glob expression. See **help glob** for a description of **glob** expression syntax.
- **key-size**
  Displays the size of the cryptographic key, in bits.
- **key-type**
  Displays the cryptographic algorithm that this key is compatible with. A key can be one of two types:
  - **rsa-private**
    The key is an RSA private key.
  - **dsa-private**
    The key is a DSA based private key.
- **last-update-time**
  Displays the time at which the key was last modified.
- **mode**
  Displays the UNIX file permissions mode for the file associated with this key. The mode is expressed in numerical form.
- **name**
  Specifies the name of the key you want to delete.
- **partition**
  Displays the partition within which the key resides.
- **recursive**
  Displays all objects of the specified type and the folder that contains the object.
- **regex**
  Displays the items that match the regular expression. The regular expression must be preceded by an at sign (@[regular expression]) to indicate that the identifier is a regular expression. See **help regex** for a description of regular expression syntax.
- **revision**
  Displays the latest revision of the key. The revision starts with 1 increments on each update.
- **security-type**
  Displays the type of security used to handle or store the key. There are four mutually exclusive options:
  - **normal**
    Indicate the key resides in a standard form on the file-system. This is the default security type.
  - **fips**
    Indicates that the key is protected by a FIPS device on the system, and is only applicable to devices with FIPS support.

- **password**
  Indicates that the key is protected by a passphrase and stored in encrypted form.
- **nethsm**
  Indicates that the key is protected by a FIPS device outside the system.

◆ **size**
Displays the size (in bytes) of the file associated with this file object.

◆ **source-path** [URL]
Displays the path to the source of the key. This option takes a URL, for example:

source-path http://cert-server/cert_store/certs/vs_132.key

source-path https://cert-server/cert_store/certs/vs_132.key

source-path
ftp://user_name:user_password@user_server/cert_store/certs/vs_132.key

◆ **system-path**
Displays the location where the key is stored on the system.

◆ **updated-by**
Displays the name of the user who last updated the key.

See Also

delete, glob, *list*, regex, *tmsh*

sniff-updates

Displays the commit ID updates that occur over the CMI communications channel

Syntax

```
run cm sniff-updates
  [-v]
```

Description

You can use the **sniff-updates** program to monitor the internal CMI communications channel for commit ID updates. The system displays each update as it arrives, one per line.

```
(1)      (2)     (3)              (4)              (5) (6)   (7)         (8)      (9)
(10)
[15:35:57] bigip1 (v0.0.0) -> device_trust_group: CID 105.105 (bigip2) at 15:34:39
FORCE_SYNC
```

Output fields: 1) Time that update arrived from network 2) Source device 3) Version of source device 4) Destination devicegroup 5) CommitId ID 6) DeviceData CommitId ID 7) CommitId originator 8) CommitId timestamp 9) FORCE_SYNC if set (nothing if not) 10) Last sync error message (nothing if last sync was successful)

Options

You can use the following option when you run the sniff-updates program:

- **-v**
  Formats the update output using fully-qualified device and device group names and exact time64_t timestamps.

See Also

run, *tmsh*

sync-status

Displays the configuration synchronization status of the local device.

Syntax

Run the **sync-status** command sequence within the **cm** module using the syntax in the following section.

Display

```
show sync-status
    field-fmt
```

Description

You can use the **sync-status** component to display the configuration synchronization status of the local device.

For information about the options that you can use with the command **show**, run the command sequence **help show**.

Example

show sync-status

Displays the configuration synchronization status of the local device:

Options

- **field-fmt**

Formats the status output in command syntax.

See Also

show, *tmsh*

traffic-group

Manages a CM traffic group.

Syntax

Manage the **traffic-group** component within the **cm** module using the syntax shown in the following sections.

Create/Modify

```
create traffic-group [name]
modify traffic-group [name]
    app-service [[string] | none]
    auto-failback-enabled [ enabled | disabled ]
    auto-failback-time [ integer ]
    description [string ]
    ha-group [string]
    ha-load-factor [ integer ]
    ha-order [ string ... ]
    mac [mac address
edit traffic-group [ [ [name] | [glob] | [regex] ] ... ]
    all-properties
    non-default-properties
```

Display

```
list traffic-group
list traffic-group [ [ [name] | [glob] | [regex] ] ... ]
show running-config traffic-group
show running-config traffic-group [ [ [name] | [glob] | [regex] ] ... ]
    all-properties
    app-service
    is-floating
    non-default-properties
    one-line
    partition
 recursive
 unit-id [integer]
show traffic-group
show traffic-group [name]
    all-properties
    failover-objects
 field-fmt
```

Delete

```
delete traffic-group [name]
```

Description

You can use the **traffic-group** component to specify the failover behavior for devices in a failover device group.

Examples

create traffic-group my_traffic_group

Creates a traffic group named **my_traffic_group**.

create traffic-group my_traffic_group ha-order { my_device }

Creates a traffic group named **my_traffic_group** with a preferred device named **my_device**.

Options

- **app-service**
  Specifies the application service to which the object belongs. The default value is **none**. **Note:** If the **strict-updates** option is **enabled** on the Application Service that owns the object, you cannot modify or delete the object. Only the Application Service can modify or delete the object.
- **auto-failback-enabled**
  Specifies whether the traffic group fails back to the default device.
- **auto-failback-time**
  Specifies the time required to fail back. The value must be within a valid range: **0** - **300** inclusive.
- **failover-objects**
  Only usable with the **show** command. Tells it to display all of the objects associated with that traffic group.
- **ha-group**
  This specifies the name of the HA group that the traffic group uses to decide the active device within the traffic group. The HA group must exist first. **Note:** This attribute is only specific to the local device i.e. not sync'ed to its peers in the traffic group.
- **ha-order**
  This list of devices specifies the order in which the devices will become active for the traffic group when a failure occurs. This list may contain zero, one or more entries up to the number of devices in the failover device group. If auto-failback enabled is set to true, this list must contain at least one entry for the auto-failback device.
- **ha-load-factor**
  Specifies a number for this traffic group that represents the load this traffic group presents to the system relative to other traffic groups. This allows the failover daemon to load balance the active traffic groups amongst the devices. The value is one by default. The value must be within a valid range: **1** - **1000** inclusive.
- **description**
  Specifies a user-defined description.
- **glob**
  Displays the items that match the glob expression. See **help glob** for a description of **glob** expression syntax.

- **is-floating**
  Indicates whether the traffic group can fail over to other devices in the device group.
- **mac**
  Specifies a MAC address for the traffic group.
- **partition**
  Displays the administrative partition within which the device group resides.
- **regex**
  Displays the items that match the regular expression. The regular expression must be preceded by an at sign (@[regular expression]) to indicate that the identifier is a regular expression. See **help regex** for a description of regular expression syntax.
- **recursive**
  Displays all objects of the specified type and the folder that contains the object.
- **unit_id**
  Displays the unit ID for the traffic group. The unit ID is set automatically when you create a traffic group. The value is between **1** and **15**.

See Also

create, *delete*, *edit*, glob, *list*, *modify*, regex, *tmsh*

trust-domain

Manages a CM trust domain by providing control of object failover.

Syntax

Manage the **trust-domain** component within the **cm** module using the syntax shown in the following sections.

Create/Modify

```
create trust-domain [name]
modify trust-domain [name]
    ca-devices [add | delete | modify | replace-all-with] {
      [ device_name | ip address ]
    }
    md5-fingerprint [string]
 name [string]
    non-ca-devices [add | delete | modify | replace-all-with] {
      [ device_name | ip address ]
    }
    password [string]
    serial [string]
    sha1-fingerprint [string]
    username [string]
```

Display

```
list trust-domain
list trust-domain [ [ [name] | [glob] | [regex] ] ... ]
show running-config trust-domain
show running-config trust-domain [ [ [name] | [glob] | [regex] ] ... ]
    all-properties
    app-service
    ca-cert
    ca-cert-bundle
    ca-key
    non-default-properties
    one-line
    partition
    recursive
 status
    trust-group
```

Delete

```
delete trust-domain all
    keep-current-certificate-authority
    import-user-defined-cert [string]
    import-user-defined-key [string]
```

Description

You can use the **trust-domain** component to manage the behavior of objects during fail over.

Examples

Adds a certificate authority:

modify trust-domain Root ca-devices add { 192.168.1.245 } name myDevice1 username admin password admin

Adds a non-authoritative certificate:

modify trust-domain Root non-ca-devices add { 192.168.1.245 } name myDevice1 username admin password admin

Removes a device from the trust domain:

modify trust-domain Root ca-devices delete { myDevice1 }

Resets the trust and makes this device standalone:

delete cm trust-domain all

Options

- **app-service**
  Displays the application service to which the object belongs. The default value is **none**. **Note:** If the **strict-updates** option is **enabled** on the Application Service that owns the object, you cannot modify or delete the object. Only the Application Service can modify or delete the object.
- **ca-cert**
  Displays the certificate authority device trust certificate.
- **ca-cert-bundle**
  Displays the bundled certificate authority device trust certificates used to authenticate incoming connections.
- **ca-devices**
  Specifies a set of certificate authority devices in the trust domain.
- **ca-key**
  Displays the certificate authority device trust key. This key only displays for certificate authorities.
- **glob**
  Displays the items that match the glob expression. See **help glob** for a description of **glob** expression syntax.
- **import-user-defined-cert**
  Specifies the certificate to import and use as the trust domain's new certificate authority. You must also use the **import-user-defined-key** option to specify the corresponding key. This option cannot be specified alongside **keep-current-certificate-authority**.

- **import-user-defined-key**
  Specifies the key to import and use as the trust domain's new certificate authority key. You must also use the **import-user-defined-cert** option to specify the corresponding certificate. This option cannot be specified alongside **keep-current-certificate-authority**.
- **keep-current-certificate-authority**
  By default, resetting trust will generate a new certificate authority. Adding this option to the **delete** command will instead keep the current certificate authority. This option cannot be specified alongside **import-user-defined-cert** or **import-user-defined-key**.
- **md5-fingerprint**
  Specifies the SSL certificate fingerprint when verifying the identity of a new device.
- **name**
  Option used to specify the name of a new device.
- **non-ca-devices**
  Specifies a set of subordinate devices in the trust domain.
- **password**
  Specifies the password for a new device.
- **recursive**
  Displays all objects of the specified type and the folder that contains the object.
- **regex**
  Displays the items that match the regular expression. The regular expression must be preceded by an at sign (@[regular expression]) to indicate that the identifier is a regular expression. See **help regex** for a description of regular expression syntax.
- **serial**
  Specifies the SSL certificate serial number when verifying the identity of a new device.
- **sha1-fingerprint**
  Specifies the SSL certificate fingerprint when verifying the identity of a new device.
- **signature**
  Specifies the SSL certificate signature, when verifying the identity of a new device.
- **status**
  Displays the status of the trust domain.
- **trust-group**
  Displays the device group associated with the trust domain.
- **username**
  Specifies the user name required to log on to a device when adding the device to the trust domain.

See Also

create, *delete*, *edit*, glob, *list*, *modify*, regex, *tmsh*

watch-devicegroup-device

Displays information about the devices in the device group to which the local device belongs.

Syntax

Run the **watch-devicegroup-device** program within the **cm** module using the syntax shown in the following sections.

Run

```
run watch-devicegroup-device
```

Display

By default, multiple devices with identical information are collapsed into a single row that displays in green. The **devices** column identifies the devices by the suffix of the configuration synchronization IP address configured on the device. For example, if the devices in a device group have the IP addresses **10.0.0.15** and **10.0.0.16**, the IDs in this column will be **15** and **16**. Use the **c** (collapse) command to deactivate/activate this behavior.

Description

You can use the **watch-devicegroup-device** program to view dynamic information about the synchronization of the devices in the device group to which the local device belongs. You can use this information to monitor or troubleshoot the devices.

For example, when you make a change to a device, the change is identified by a commit ID (cid.id) that displays when you run the **watch-devicegroup-device** program.

Within the program, you can use the following keys:

- Press **h** to see a list of available commands.
- Press the back tick key (`) to exit the help page.
- Press **c** to toggle the view from a collapsed view to a full view. The command gathers information from every device in the trust group. When all devices in the trust group report the same information the view is collapsed and one line, highlighted in green, displays the information. The devices included in the line are shown in the devices column. You can press **c** to see the full view, which displays each device on a separate line.

- Press **Ctrl-C** to exit the program.
- Press the arrow keys to navigate across the columns or down the rows.

The content in the columns includes:

- **devices**
  Displays the suffix of the configuration synchronization IP address configured on the device. For example, if the devices in a device group have the config-sync IP addresses **10.0.0.15** and **10.0.0.16**, the IDs in this column will be **15** and **16**.
- **devgroup**
  Displays the name of the device group to which the device belongs.
  Note: This can be a sync-only, failover, or trust device group.
- **device**
  Displays the device object name.
- **cid.id**
  Displays the commit ID, which is a configuration change identifier.
- **cid-orig**
  Displays the name of the device on which the configuration change was made.
- **cid.time**
  Displays the time the configuration change was made.
- **last_sync**
  Displays the time the device configuration was last synchronized with the device group.
  The devices in the **to-group** of a configuration synchronization display the same time in this column. The local device that pushes the configuration to the other devices in the device group (to-group) has a different value in this column.
  The devices in the **from-group** of a configuration synchronization display the same time in this column. The local device that receives the configuration from the other devices has a different value in this column. You can use this information to determine a rollback strategy.

See Also

run, *tmsh*, *watch-sys-device*, *watch-trafficgroup-device*

watch-sys-device

Displays information about the local device.

Syntax

Run the **watch-sys-device** program within the **cm** module using the syntax shown in the following sections.

Run

```
run watch-sys-device
```

Display

By default, multiple devices with identical information are collapsed into a single row that displays in green. The **devices** column identifies the devices by the suffix of the configuration synchronization IP address configured on the device. For example, if the devices in a device group have the IP addresses **10.0.0.15** and **10.0.0.16**, the IDs in this column will be **15** and **16**. Use the **c** (collapse) command to deactivate/activate this behavior.

Description

You can use the **watch-sys-device** program to view dynamic information about the local device.

Within the program, you can use the following keys:

- Press **h** to see a list of available commands.
- Press the back tick key (`) to exit the help page.
- Press **c** to toggle the view from a collapsed view to a full view. The command gathers information from every device in the trust group. When all devices in the trust group report the same information the view is collapsed and one line, highlighted in green, displays the information. The devices included in the line are shown in the devices column. You can press **c** to see the full view, which displays each device on a separate line.
- Press **Ctrl-C** to exit the program.
- Press the arrow keys to navigate across the columns or down the rows.

The content in the columns includes:

- **devices**
  Displays the suffix of the configuration synchronization IP address configured on the device. For example, if the devices in a device group have the IP addresses **10.0.0.15** and **10.0.0.16**, the IDs in this column will be **15** and **16**.
- **name**
  Displays the device object name.
- **platform**
  Displays the device platform.
- **build**
  Displays the software build installed on the device.
- **failover_state**
  Displays the high availability state (active or standby) of the device.
- **mgmt_ip**
  Displays the IP address of the management port on the device.
- **configsync_ip**
  Displays the IP address on the device that is used for configuration synchronization.
- **unicast_ip**
  Displays the unicast IP address of the device.
- **multicast_ip**
  Displays the multicast IP address of the device.
- **mirror_ip**
  Displays the IP address used for configuration mirroring for the device.
- **mirror_secondary_ip**
  Displays the secondary IP address used for configuration mirroring for the device.
- **desc**
  Displays a description of the device.

See Also

run, *tmsh*, *watch-devicegroup-device*, *watch-trafficgroup-device*

watch-trafficgroup-device

Displays information about the traffic groups associated with devices in a device group.

Syntax

Run the **watch-trafficgroup-device** program within the **cm** module using the syntax shown in the following sections.

Run

```
run watch-trafficgroup-device
```

Display

By default, multiple devices with identical information are collapsed into a single row that displays in green. The **devices** column identifies the devices by the suffix of the configuration synchronization IP address configured on the device. For example, if the devices in a device group have the IP addresses **10.0.0.15** and **10.0.0.16**, the IDs in this column will be **15** and **16**. Use the **c** (collapse) command to deactivate/activate this behavior.

Description

You can use the **watch-trafficgroup-device** program to view dynamic information about the failover status of the devices in a device group to which the local device belongs. You can use this information to monitor or troubleshoot the devices in the device group.

Within the program, you can use the following keys:

- Press **h** to see a list of available commands.
- Press the back tick key (`) to exit the help page.
- Press **c** to toggle the view from a collapsed view to a full view. The command gathers information from every device in the device group. When all devices in the device group report the same information the view is collapsed and one line, highlighted in green, displays the information. The devices included in the line are shown in the devices column. You can press **c** to see the full view, which displays each device on a separate line.
- Press **Ctrl-C** to exit the program.
- Press the arrow keys to navigate across the columns or down the rows.

The content in the columns includes:

- **devices**
  Displays the suffix of the configuration synchronization IP address configured on the device. For example, if the devices in a device group have the IP addresses **10.0.0.15** and **10.0.0.16**, the IDs in this column will be **15** and **16**.
- **traffic_group**
  Displays the name of the traffic group associated with the device.
- **device_name**
  Displays the device object name.
- **failover_state**
  Displays the high availability state (active or standby) of the device.
- **next_active**
  Displays **True** for the device that becomes active if the active traffic group fails over.
- **score**
  Displays a system-generated high availability score used to select the next active device.

See Also

run, *tmsh*, *watch-sys-device*, *watch-devicegroup-device*

46

gtm

- Introducing the gtm module
- Alphabetical list of components

Introducing the gtm module

You can use the tmsh components that reside within the gtm module to configure Global Traffic Manager™. For more information about the tmsh hierarchical structure, see Chapter 2, *Understanding and Using the Traffic Management Shell*.

Alphabetical list of components

The remainder of this chapter lists the tmsh components that are available in the gtm module.

datacenter

Configures a Global Traffic Manager™ data center.

Syntax

Configure the **datacenter** component within the **gtm** module using the syntax in the following sections.

Create/Modify

```
create datacenter [name]
modify datacenter [name]
    app-service [[string] | none]
    contact [ [name] | none]
    description [string]
    [disabled | enabled]
    location [none | [physical location] ]
    prober-pool [none | name]
    metadata
      [add | delete | modify] {
        [metadata_name ... ] {
          value [ "value content" ]
          persist [ true | false ]
        }
    }
edit datacenter [ [ [name] | [glob] | [regex] ] ... ]
    all-properties
    non-default-properties
    one-line
reset-stats datacenter
reset-stats datacenter [ [ [name] | [glob] | [regex] ] ... ]
```

Display

```
list datacenter
list datacenter [ [ [name] | [glob] | [regex] ] ... ]
show running-config datacenter
show running-config datacenter [ [ [name] | [glob] | [regex] ] ... ]
    all-properties
    non-default-properties
show datacenter
show datacenter [name]
    (default | exa | gig | kil | meg | peta | raw | tera | yotta | zetta)
    detail
    field-fmt
```

Delete

```
delete datacenter [name]
```

Description

You can use the **datacenter** component to create, modify, display, or delete a data center.

Examples

create datacenter DC1

Creates a data center named DC1 with options set to the default values.

list datacenter DC1 all-properties

Displays all properties of the data center named DC1.

Options

- **app-service**
  Specifies the name of the application service to which the data center belongs. The default value is **none**. **Note:** If the **strict-updates** option is **enabled** on the application service that owns the object, you cannot modify or delete the data center. Only the application service can modify or delete the data center.
- **contact**
  Specifies the name of the administrator or the name of the department that manages the data center. The default value is **none**.
- **description**
  User defined description.
- **[disabled | enabled]**
  Specifies whether the data center and its resources are available for load balancing. The default value is **enabled**.
- **glob**
  Displays the items that match the **glob** expression. See **help glob** for a description of **glob** expression syntax.
- **location**
  Specifies the physical location of the data center. The default value is **none**.
- **metadata**
  Specifies user-defined data to associate with a server. By default the **persist** attribute is set to **true**. This means the data is saved into the configuration file.
- **name**
  Specifies a unique name for the component. This option is required for the commands **create** and **modify**.
- **prober-pool**
  Specifies a prober pool to use to monitor servers defined in this data center.

- **regex**
  Displays the items that match the regular expression. The regular expression must be preceded by an at sign (@[regular expression]) to indicate that the identifier is a regular expression. See **help regex** for a description of regular expression syntax.

See Also

create, *delete*, glob, *link*, *prober-pool*, *server*, *list*, *modify*, regex, *reset-stats*, *show*, *tmsh*

distributed-app

Configures a Global Traffic Manager™ distributed application.

Syntax

Configure the **distributed-app** component within the **gtm** module using the syntax in the following sections.

Create/Modify

```
create distributed-app [name]
modify distributed-app [name]
   app-service [[string] | none]
   dependency-level [datacenter | link | none | server | wideip]
   description [string]
   disabled-contexts
     [add | delete | modify | replace-all-with] {
       [datacenter | link | server] [name] ...
   }
   disabled-contexts none
   persistence [enabled | disabled]
   persist-cidr-ipv4 [integer]
   persist-cidr-ipv6 [integer]
   ttl-persistence [integer]
   wideips
     [add | delete | replace-all-with] {
       [name] ...
   }
   wideips [default | none]
edit distributed-app
  [ [ [name] | [glob] | [regex] ] ... ]
   all-properties
   non-default-properties
   one-line
reset-stats distributed-app
reset-stats distributed-app
  [ [ [name] | [glob] | [regex] ] ... ]
```

Display

```
list distributed-app
list distributed-app [ [ [name] | [glob] | [regex] ] ... ]
show running-config distributed-app
show running-config distributed-app
  [ [ [name] | [glob] | [regex] ] ... ]
  all-properties
  non-default-properties
  partition
show distributed-app
show distributed-app [name]
  (default | exa | gig | kil | meg | peta | raw | tera | yotta | zetta)
  detail
  field-fmt
```

Delete

```
delete distributed-app [name]
```

Description

You can use the **distributed-app** component to create, modify, display, or delete a distributed application.

Examples

create distributed-app DA1

Creates a distributed application named DA1 with options set to the default values.

list distributed-app DA1 all-properties

Displays all properties of the distributed application named DA1.

Options

- **app-service**
  Specifies the name of the application service to which the distributed application belongs. The default value is **none**. **Note:** If the **strict-updates** option is **enabled** on the application service that owns the object, you cannot modify or delete the distributed application. Only the application service can modify or delete the distributed application.
- **dependency-level**
  Specifies the resources that must be in the available state before this distributed application is considered available. The options are:
  - **datacenter**
    All of the data centers on the member list of this distributed application must be in an available state before the system considers the distributed application available.
  - **link**
    All of the links on the member list of this distributed application must be in an available state before the system considers the distributed application available.
  - **none**
    The distributed application has no dependencies. This value effectively disables this option. This is the default value.
  - **server**
    All of the servers on the member list of this distributed application must be in an available state before the system considers the distributed application available.

- **wideip**
  All of the wideips on the member list of this distributed application must be in an available state before the system considers the distributed application available.

- **description**
  User defined description.
- **disabled-contexts**
  Specifies the components that you want to add to or delete from this distributed application as disabled-contexts. You can also replace all of the components that are currently listed as disabled-contexts for this distributed application with other components. The default value is **none**. The possible values are:
  - **datacenter**
    Specifies the datacenters, by name, to which the system does not send traffic from this distributed application.
  - **link**
    Specifies the links, by name, to which the system does not send traffic from this distributed application.
  - **none**
    There are no components to which the system does not send traffic from this distributed application. This value effectively disables this option.
  - **server**
    Specifies the servers, by name, to which the system does not send traffic from this distributed application.
- **glob**
  Displays the items that match the **glob** expression. See **help glob** for a description of **glob** expression syntax.
- **name**
  Specifies a unique name for the component. This option is required for the commands **create** and **modify**.
- **partition**
  Displays the administrative partition within which this object resides.
- **persistence**
  When **enabled**, if a local DNS server makes repetitive requests on behalf of a client, the system reconnects the client to the same resource as previous requests. The default value is **disabled**.
- **persist-cidr-ipv4**
  Specifies a mask used to group IPv4 LDNS addresses. This feature allows one persistence record to be shared by LDNS addresses that match within this mask.
- **persist-cidr-ipv6**
  Specifies a mask used to group IPv6 LDNS addresses. This feature allows one persistence record to be shared by LDNS addresses that match within this mask.

- **regex**
  Displays the items that match the regular expression. The regular expression must be preceded by an at sign (@[regular expression]) to indicate that the identifier is a regular expression. See **help regex** for a description of regular expression syntax.
- **ttl-persistence**
  Specifies, in seconds, the length of time for which the persistence entry is valid. The default value is **3600**.
- **wideips**
  Specifies the wide IPs, by name, that you want to add to or delete from this distributed application. You can also replace all of the wide IPs that are currently associated with this distributed application with other wide IPs. The default value is **none**.
  A wide IP is a collection of one or more domain names that maps to one or more groups of virtual servers managed either by BIG-IP® systems, or by host servers. The Global Traffic Manager load balances name resolution requests across the virtual servers that are defined in the wide IP that is associated with the requested domain name.

See Also

create, *delete*, glob, *link*, *server*, *create*, *list*, *modify*, regex, *reset-stats*, *show*, *tmsh*

iquery

Displays information about iQuery.

Syntax

Display the **iquery** component within the **gtm** module using the syntax in the following sections.

Display

```
show iquery
    (default | exa | gig | kil | meg | peta | raw | tera | yotta | zetta)
    field-fmt
    global
```

Description

You can use the **iquery** component to display iQuery statistics.

Examples

show iquery

Displays iQuery statistics in the system default units.

show iquery field-fmt

Displays iQuery statistics in field format.

Options

For information about options for the command **show**, see **show**.

See Also

show, *tmsh*

ldns

Displays local domain name system (LDNS) statistics for the Global Traffic Manager™.

Syntax

Display the **ldns** component within the **gtm** module using the syntax in the following section.

Display

```
show ldns
    (default | exa | gig | kil | meg | peta | raw | tera | yotta | zetta)
    field-fmt
```

Description

You can use the **ldns** component to display LDNS statistics.

Examples

show ldns

Displays LDNS statistics in the system default units.

show ldns field-fmt

Displays LDNS statistics in field format.

See Also

show, *tmsh*

link

Configures Global Traffic Manager™ links.

Syntax

Configure the **link** component within the **gtm** module using the syntax in the following sections.

Create/Modify

```
create link [name]
modify link [name]
    app-service [[string] | none]
    cost-segments {
       { [up-to-bps [integer] ] [dollars-per-mbps [integer] ] }...
    }
    datacenter [string]
    description [string]
    [disabled | enabled]
    duplex-billing [disabled | enabled]
    limit-max-inbound-bps [integer]
    limit-max-inbound-bps-status [disabled | enabled]
    limit-max-outbound-bps [integer]
    limit-max-outbound-bps-status [disabled | enabled]
    limit-max-total-bps [integer]
    limit-max-total-bps-status [disabled | enabled]
    link-ratio [integer]
    monitor [ [name] | none]
    prepaid-segment [integer]
    router-addresses
      [add | delete | modify | replace-all-with] {
        [ip address] {
          app-service [[string] | none]
          translation [disabled | enabled]
          device-name [name]
        }
    }
    service-provider [name]
    uplink-address [ip address]
    weighting [price | ratio]
edit link [ [ [name] | [glob] | [regex] ] ... ]
    all-properties
    non-default-properties
    one-line
reset-stats link
reset-stats link [ [ [name] | [glob] | [regex] ] ... ]
```

Display

```
list link
list link [ [ [name] | [glob] | [regex] ] ... ]
show running-config link
show running-config link [ [ [name] | [glob] | [regex] ] ... ]
    all-properties
    non-default-properties
```

```
show link
show link [name]
    (default | exa | gig | kil | meg | peta | raw | tera | yotta | zetta)
    detail
    field-fmt
```

Delete

```
delete link [name]
```

Description

You can use the link component to create, display, modify, or delete a link.

A link is a physical device that connects the network to the rest of the Internet. You can logically attach links to a collection of servers in order to manage access to the data sources on the network.

Examples

create link my_link datacenter DC1 router-addresses add {10.10.1.1}

Creates a link named **my_link** in the **DC1** data center and adds the IP address of the router that uses this link.

list link non-default-properties

Displays all non-default properties for all links.

delete link my_link

Deletes the link named **my_link**.

show link *my_link* **detail**

Show the servers and virtual servers associated with *my_link*.

show link all detail

Show the servers and virtual servers associated with each respective link in the system.

Options

- **app-service**
  Specifies the name of the application service to which the link belongs. The default value is **none**. **Note:** If the **strict-updates** option is **enabled** on the application service that owns the object, you cannot modify or delete the link. Only the application service can modify or delete the link.
- **cost-segments**
  Specifies the cost of each incremental segment of bandwidth. This option is valid only when the **weighting** option is set to **price**. Note that you cannot modify the list, only replace all of the options in the list.
  By default, the list is empty. The options are:

- **dollars-per-mps**
  Specifies the cost in dollars per megabytes per second. By default this value is not specified.
- **up-to-bps**
  Specifies the cost in dollars per bytes per second. By default this value is not specified.

◆ **datacenter**
Specifies the data center to which the link belongs.

◆ **description**
User defined description.

◆ **detail**
The **detail** option is used with the **show** display command. This shows the server IP addresses and virtual servers associated with this link. A server can have multiple server IP addresses, however, only the server IP addresses that use this link will be displayed. Assignment information for servers and virtuals will not be displayed if there are not any servers or virtuals that use this link. By default, links are automatically matched to server IP addresses and virtual servers according to their IP addresses. Explicit links may also be defined. How this link was assigned is displayed under the Link Assignment column: **auto** means that the system automatically assigned this link, and **explicit** means that the link was explicitly set by the user.

◆ **[disabled | enabled]**
Specifies whether the link and its resources are available for load balancing. The default value is **enabled**.

◆ **duplex-billing**
Enables or disables duplex billing for this link. The default value is **enabled**. This option is valid only when the **weighting** option is set to **price**.

- **disabled**
  The internet service provider (ISP) that supplies this link bills for bandwidth usage based on the total amount of inbound plus outbound traffic on the link.
- **enabled**
  The ISP that supplies this link bills for bandwidth usage based on the maximum amount of either inbound or outbound traffic on the link (whichever is higher), rather than billing for bandwidth usage based on the total amount of inbound plus outbound traffic on the link.

◆ **glob**
Displays the items that match the **glob** expression. See **help glob** for a description of **glob** expression syntax.

◆ **limit-max-inbound-bps**
Specifies the threshold for inbound traffic on the link. The default value is **0** (zero).

◆ **limit-max-inbound-bps-status**
Enables or disables the **limit-max-inbound-bps** option for this link. The default value is **disabled**.

- **limit-max-outbound-bps**
  Specifies the threshold for inbound traffic on the link. The default value is **0** (zero).
- **limit-max-outbound-bps-status**
  Enables or disables the **limit-max-outbound-bps** option for this link. The default value is **disabled**.
- **limit-max-total-bps**
  Specifies the threshold as a sum of inbound and outbound traffic on the link. The default value is **0** (zero).
- **limit-max-total-bps-status**
  Enables or disables the **limit-max-total-bps** option for this link. The default value is **disabled**.
- **link-ratio**
  Specifies the frequency at which the system sends traffic through the link. The default value is **1**.

Important

*When you set this option, you must also set the **weighting** option to **ratio**.*

- **monitor**
  Specifies the health monitors that the system uses to determine whether this link is available for load balancing. The default value is **none**.
- **name**
  Specifies a unique name for the component. This option is required for the commands **create** and **modify**.
- **prepaid-segment**
  Specifies the amount of bandwidth for which the system is prepaid. This option is valid only when the **weighting** option is set to **price**. The default value is **0** (zero).
- **regex**
  Displays the items that match the regular expression. The regular expression must be preceded by an at sign (@[regular expression]) to indicate that the identifier is a regular expression. See **help regex** for a description of regular expression syntax.
- **router-addresses**
  Specifies the IP addresses of the routers that use this link. A router address can be associated with only one link. You can use the following options:
  - **app-service**
    Specifies the name of the application service to which the link belongs. The default value is **none**. **Note:** If the **strict-updates** option is **enabled** on the application service that owns the object, you cannot modify or delete the link. Only the application service can modify or delete the link.

  - **translation**
    Specifies the address that the link uses for translation when communicating between the network and the Internet. The default value is **any6**.
  - **device-name**
    Specifies the name of this system in a redundant system. The default value is the link name.
- **service-provider**
  Specifies the Internet Service Provider (ISP) or vendor that supplies this link. This allows you to provide a name or description that helps identify this link out of your data center. This is an optional field.
- **uplink-address**
  Specifies the IP address the system uses to gather Simple Network Management Protocol (SNMP) metrics from the router interface. When you configure an uplink address, the system sends SNMP requests to the IP addresses configured using the **router-addresses** option for this link.
- **weighting**
  Specifies the weighting methodology the system uses to select a link to which to send traffic. The default value is **ratio**. The options are:
  - **price**
    The system continuously checks the performance of each link, and sends traffic through the link with the best performance data.
  - **ratio**
    The system uses the value that you set in the **link-ratio** option to determine the link to which to send traffic.

See Also

create, *delete*, *edit*, glob, *datacenter*, *server*, *list*, *modify*, regex, *reset-stats*, *show*, *tmsh*

listener

Configures a Global Traffic Manager™ listener.

Syntax

Configure the **listener** component within the **gtm** module using the syntax in the following sections.

Create/Modify

```
create listener [name]
modify listener [name]
    address [ip address]
    advertise [yes | no]
    app-service [[string] | none]
    auto-lasthop [default | enabled | disabled ]
    description [string]
    [disabled | enabled]
    fallback-persistence [none | [profile name] ]
    ip-protocol [tcp | udp]
    last-hop-pool [ [pool_name] | none]
    mask { [ipv4] | [ipv6] }
    persist [replace-all-with] {
        [profile_name ... ] {
            default [no | yes]
        }
    }
    persist none
    pool [ [pool_name] | none]
    port [service port]
    profiles [add | delete | replace-all-with] {
        [profile name ...] {
           context [all | clientside | serverside]
        }
    }
    rules { [none | [rule_name ... ] }
    source-address-translation {
        pool [ [pool_name] | none]
        type [ automap | snat | none ]
    }
    source-port [change | preserve | preserve-strict]
    translate-address [enabled | disabled]
    translate-port [enabled | disabled]
    vlans none
    vlans
      [ add | delete | replace-all-with ] {
        [vlan name]...
    }
    vlans-disabled
    vlans-enabled
edit listener [ [ [name] | [glob] | [regex] ] ... ]
    all-properties
    non-default-properties
    one-line
reset-stats listener
reset-stats listener [ [ [name] | [glob] | [regex] ] ... ]
```

Display

```
list listener
list listener [name]
show running-config listener
show running-config listener [ [ [name] | [glob] | [regex] ] ... ]
    all-properties
    non-default-properties
    partition
show listener
show listener [name]
    (default | exa | gig | kil | meg | peta | raw | tera | yotta | zetta)
    field-fmt
```

Delete

```
delete listener [name]
```

Description

You can use the **listener** component to create, display, modify, or delete a listener.

A listener is an object that listens for DNS queries. Listeners are defined for specific IP addresses, and are always associated with port **53**.

Important

When you create, modify, or delete a listener, the system saves the running configuration in the stored configuration files.

Examples

create listener my_listener address 10.10.1.1 persist replace-all-with { source_addr }

Creates a listener named **my_listener** with an IP address of **10.10.1.1**, which uses the source address persistence method.

modify listener my_listener profiles replace-all-with { dns }

Replaces the profiles associated with the listener **my_listener**.

Note

To replace the profile associated with a listener, you must enclose the name of the new profile in curly brackets.

list listener non-default-properties

Displays all non-default properties for all listeners.

delete listener my_listener

Deletes the listener named **my_listener**.

Options

- **address**
  Specifies the IP address on which the system listens. The system receives traffic sent to this IP address and processes it as needed. This option is required.
- **advertise**
  Specifies whether to advertise the listener address to surrounding routers. The options are **yes** or **no**. The default value is **no**.
- **app-service**
  Specifies the name of the application service to which the listener belongs. The default value is **none**. **Note:** If the **strict-updates** option is **enabled** on the application service that owns the object, you cannot modify or delete the listener. Only the application service can modify or delete the listener.
- **context**
  Specifies that the protocol profile is either a **clientside** or **serverside** profile. If not specified, the default value is **all** for both sides.
- **description**
  User defined description.
- **(enabled | disabled)**
  Specifies the state of the listener. The default value is **enabled**.

◆ Note

*When you disable a listener, the listener no longer accepts new connection requests. However, it allows current connections to finish processing before going to a **down** state.*

- **fallback-persistence**
  Specifies a fallback persistence profile for the listener to use when the default persistence profile is not available. The default value is **none**.
- **glob**
  Displays the items that match the **glob** expression. See **help glob** for a description of **glob** expression syntax.
- **ip-protocol**
  Specifies the protocol on which this listener receives network traffic. The options are **udp** or **tcp**. The default value is **udp**.
- **last-hop-pool**
  Specifies the name of the last hop pool that you want the listener to use to direct reply traffic to the last hop router. The default value is **none**.
- **mask**
  Specifies the netmask for a network listener only. This setting is required for a network listener.
  The netmask clarifies whether the host bit is an actual zero or a wildcard representation. The default value is **255.255.255.255** for IPv4 or **ffff:ffff:ffff:ffff:ffff:ffff:ffff:ffff** for IPv6.

- **name**
  Specifies a unique name for the component. This option is required for the commands **create** and **modify**.
- **partition**
  Displays the administrative partition within which the listener resides.
- **persist**
  Specifies a list of profiles separated by spaces that the listener uses to manage connection persistence. The default value is **none**.
  To enable persistence, typically you specify a single profile. However, you can specify multiple profiles in conjunction with iRules® that define a persistence strategy based on incoming traffic. In the case of multiple profiles, the **default** option specifies which profile you want the listener to use if an iRule does not specify a persistence method. When you specify multiple profiles, the default value of the default property is **no**. You can set the value of the **default** property to **yes** for only one of the profiles.
- **pool**
  Specifies a default pool to which you want the listener to automatically direct traffic. The default value is none.
- **port**
  Specifies the service port on which the listener listens for connections. When you create a listener, the default value is 53 if no port number is specified.
- **profiles**
  Specifies the DNS, statistics and protocol profiles to use for this listener. When a listener is created, if a DNS profile is not specified, the generic "dns" profile is added. If a protocol profile is not specified, then the generic "tcp" profile is added for TCP and the "udp_gtm_dns" profile is added for UDP. A listener always has DNS and protocol profiles once it is created. Only a statistics profile can be added to or deleted from a listener.
  The **replace-all-with** command replaces the profiles with the specified ones. The unspecified DNS and protocol profiles are not changed. If statistics profiles are not specified, the **replace-all-with** command removes the existing statistics profile from the listener. When the protocol is modified, if profiles are not specified, a default protocol profile is used. DNS and statistics profiles will not change.
- **rules**
  Specifies a list of iRules, separated by spaces, that customize the listener to direct and manage traffic. The default value is **none**.
- **regex**
  Displays the items that match the regular expression. The regular expression must be preceded by an at sign (@[regular expression]) to indicate that the identifier is a regular expression. See **help regex** for a description of regular expression syntax.
- **source-address-translation**
  Specifies the type of source address translation enabled for the listener as well as the pool that the source address translation will use.

- **pool**
  Specifies the name of a SNAT pool used by the specified listener.
- **type**
  Specifies the type of source address translation associated with the specified listener.
  The options are:
  - **automap**
    Specifies the use of self IP addresses for listener source address translation.
  - **none**
    Specifies no source address translation to be used by the listener.
  - **snat**
    Specifies the use of a SNAT pool of translation addresses for listener source address translation.

◆ **source-port**
Specifies whether the system preserves the source port of the connection. The default value is **preserve**.
The options are:

- **change**
  Obfuscates internal network addresses.
- **preserve**
  Preserves the source port of the connection.
- **preserve-strict**
  Use this value only for UDP under very special circumstances, such as nPath or transparent (that is, no translation of any other L3/L4 field), where there is a 1:1 relationship between virtual IP addresses and node addresses, or when clustered multi-processing (CMP) is disabled.

◆ **translate-address**
Enables or disables address translation for the listener. Disable address translation for a listener if you want to use the listener to load balance connections to any address. This option is useful when the system is load balancing devices that have the same IP address. The default value is **disabled**.

◆ **translate-port**
Enables or disables port translation. Disable port translation for a listener, if you want to use the listener to load balance connections to any service. The default value is **disabled**.

◆ **vlans**
Specifies a list of VLANs on which traffic is either disabled or enabled, based on whether the **vlans-disabled** or **vlans-enabled** option is specified.

◆ **vlans-disabled**
Specifies that traffic is not accepted by this listener on the VLANs specified in the **vlans** option. This option is mutually exclusive with the **vlans-enabled** option.

- **vlans-enabled**
  Specifies that traffic is accepted by this listener on only the VLANs specified in the **vlans** option. This option is mutually exclusive with the **vlans-disabled** option.

See Also

create, *delete*, *edit*, glob, *list*, *modify*, *vlan*, *vlan-group*, regex, *reset-stats*, *show*, *tmsh*

path

Displays or resets path statistics for the Global Traffic Manager™.

Syntax

Configure the **path** component within the **gtm** module using the syntax in the following section.

Display

```
show path
    (default | exa | gig | kil | meg | peta | raw | tera | yotta | zetta)
    field-fmt
```

Description

You can use the **path** component to display path statistics for the Global Traffic Manager. You can also reset the path statistics to zero at any time.

See Also

show, *tmsh*

persist

Displays persistence records for the Global Traffic Manager™.

Syntax

Display statistics for the **persist** component within the **gtm** module using the syntax in the following section.

Display

```
show persist
    destination [ [destination] | none]
    level [application | wideip]
    max-results [integer]
    target-name [ [name] | none]
    target-type [datacenter | link | pool-member | server]
    value [ip address | string]
```

Description

You can use the **persist** component to display various persistence records based on the filtering options that you use.

Examples

show persist

Displays all Global Traffic Manager persistence records.

show persist level link

Displays persistence records only for links.

Options

- **destination**
  Displays persistence records for the specified destination.
- **ldns**
  Displays persistence records for the specified LDNS address.
- **level**
  Displays persistence records for the specified level (destination type).
- **max-results**
  Specifies the maximum number of persistence records that you want the system to return.
- **target-name**
  Displays persistence records for the specified target.

- **target-type**
  Displays persistence records for the specified type of target.

See Also

show, *tmsh*

pool

Configures load balancing pools for the Global Traffic Manager™.

Syntax

Modify the Global Traffic Manager **pool** component within the **gtm** module using the syntax shown in the following sections.

Create/Modify

```
create pool [name]
modify pool [name]
  alternate-mode [drop-packet | fallback-ip | global-availability
    | none | packet-rate | ratio | return-to-dns | round-robin
    | static-persistence | topology | virtual-server-capacity
    | virtual-server-score]
  app-service [[string] | none]
  canonical-name [name]
  description [string]
  [disabled | enabled]
  dynamic ratio [disabled | enabled]
  fallback-ipv4 [ip address]
  fallback-ipv6 [ip address]
  fallback-mode [completion-rate | cpu | drop-packet | fallback-ip
    | fewest-hops | global-availability | kilobytes-per-second
    | least-connections | lowest-round-trip-time | none
    | packet-rate | quality-of-service | ratio | return-to-dns
    | round-robin | static-persistence | topology
    | virtual-server-capacity | virtual-server-score]
  limit-max-bps [integer]
  limit-max-bps-status [disabled | enabled]
  limit-max-connections [integer]
  limit-max-connections-status [disabled | enabled]
  limit-max-pps [integer]
  limit-max-pps-status [disabled | enabled]
  load-balancing-mode [completion-rate | cpu | drop-packet
    | fallback-ip | fewest-hops | global-availability
    | kilobytes-per-second | least-connections
    | lowest-round-trip-time | packet-rate | quality-of-service
    | ratio | return-to-dns | round-robin | static-persistence
    | topology | virtual-server-capacity | virtual-server-score]
  manual-resume [disabled | enabled]
  max-addresses-returned [integer]
  members none
  members
    [ add | delete | modify | replace-all-with ] {
      [vs-name] {
          app-service [[string] | none]
          depends-on none
          depends-on
            [ add | delete | replace-all-with ] {
              [vs-name]...
          }
          description [string]
          [disabled | enabled]
          limit-max-bps [integer]
```

```
            limit-max-bps-status [disabled | enabled]
            limit-max-connections [integer]
            limit-max-connections-status [disabled | enabled]
            limit-max-pps [integer]
            limit-max-pps-status [disabled | enabled]
            load-balancing-mode
            monitor [disabled | enabled]
            order [integer]
            ratio
        }...
    }
    metadata
      [add | delete | modify] {
        [metadata_name ... ] {
          app-service [[string] | none]
          value [ "value content" ]
          persist [ true | false ]
        }
    }
    monitor [name]
    qos-hit-ratio [integer]
    qos-hops [integer]
    qos-kilobytes-second [integer]
    qos-lcs [integer]
    qos-packet-rate [integer]
    qos-rtt [integer]
    qos-topology [integer]
    qos-vs-capacity [integer]
    qos-vs-score [integer]
    ttl [integer]
    verify-member-availability [disabled | enabled]
  edit pool [ [ [name] | [glob] | [regex] ] ... ]
    all-properties
    non-default-properties
  reset-stats pool
  reset-stats pool [ [ [name] | [glob] | [regex] ] ... ]
```

Display

```
  list pool
  list pool [ [ [name] | [glob] | [regex] ] ... ]
  show running-config pool
  show running-config pool [ [ [name] | [glob] | [regex] ] ... ]
    all-properties
    non-default-properties
    members vs-name
    one-line
    partition
  show pool
  show pool [name]
    (default | exa | gig | kil | meg | peta | raw | tera | yotta | zetta)
    detail
    field-fmt
```

Delete

```
delete pool [name]
```

◆ Note

You must remove all references to a pool before you can delete the pool.

Description

You can use the pool component to configure the pool definitions on the Global Traffic Manager. You use a pool to group member servers together to use a common load balancing algorithm.

Examples

create pool mypool members add {
member myServer:myVs
member 10.2.3.12:http
}
monitor all http

Creates a Global Traffic Manager pool with two members **myServer:myVs**, and **10.2.3.12**, where both members use the Round Robin load balancing method, and the default HTTP monitor checks for member availability.

delete pool my_pool

Deletes the pool **my_pool**.

show pool

Displays statistics for all pools.

list pool my_pool

Displays settings of pool **my_pool**.

Options

- **alternate-mode**
  Specifies the load balancing mode that the system uses to load balance name resolution requests among the members of this pool, if the preferred method is unsuccessful in picking a pool. You set the preferred mode using the **load-balancing-mode** option. The default value is **round-robin**.
  The options are:
  - **drop-packet**
    Specifies that the Global Traffic Manager does nothing with the packet, and simply drops the request.

- **fallback-ip**
  Specifies that the Global Traffic Manager returns the IP address that you specify as an answer to the query.
- **global-availability**
  Specifies that the Global Traffic Manager distributes connection requests to virtual servers included in the pool in the order in which they are listed.
- **none**
  Specifies that the system skips the alternate load balancing mode and immediately tries the load balancing mode specified in the **fallback-mode** option.
  Note that if the value of the **fallback-mode** option is **none**, and you have multiple pools configured, the Global Traffic Manager uses the next available pool.
- **packet-rate**
  Specifies that the Global Traffic Manager assigns connection requests to the virtual server that is currently processing the fewest number of packets per second.
- **ratio**
  Specifies that the Global Traffic Manager distributes connection requests among a pool of virtual servers using a weighted Round Robin load balancing method.
- **return-to-dns**
  Specifies that the Global Traffic Manager immediately returns connection requests to the Local DNS for resolution.
- **round-robin**
  Specifies that the Global Traffic Manager distributes connection requests in a circular and sequential pattern among the virtual servers in a pool.
- **static-persistence**
  Specifies that the Global Traffic Manager consistently maps an LDNS IP address to the same available virtual server for the duration of a session.
- **topology**
  Specifies that the Global Traffic Manager uses proximity-based load balancing to distribute connection requests.
- **virtual-server-capacity**
  Specifies that the Global Traffic Manager assigns connection requests to virtual servers based on a user-defined ranking system.
- **virtual-server-score**
  Specifies that the Global Traffic Manager assigns connection requests to virtual servers based on a user-defined ranking system.

◆ **app-service**
Specifies the name of the application service to which this pool belongs. The default value is **none**. **Note:** If the **strict-updates** option is **enabled** on the application service that owns the object, you cannot modify or delete this pool. Only the application service can modify or delete this pool.

- **canonical-name**
  Specifies the canonical name of the zone, for example, **www.siterequest.com**, that the system uses for CNAME dynamic delegation. The default value is **none**.
- **description**
  User defined description.
- **[disabled | enabled]**
  Specifies whether this pool is available for load balancing. The default value is **enabled**.
- **dynamic-ratio**
  Enables or disables a dynamic ratio load balancing algorithm for this pool. This option is applicable only when you also configure the **load-balancing-mode** option for the pool with one of these dynamic load balancing modes: **completion-rate**, **fewest-hops**, **kilobytes-per-second**, **least-connections**, **lowest-round-trip-times**, **quality-of-service**, **virtual-server-capacity**, or **virtual-server-score**. When this option is **disabled** (the default), the system uses only the server or virtual server with the best metrics, or highest quality of service (QoS) score, for load balancing. When **dynamic-ratio** is **enabled**, the system treats QoS scores as ratios, and it uses each server or virtual server in proportion to the ratio determined by the QoS calculation.
- **fallback-ipv4**
  Specifies the IPv4 address of the server to which the system directs requests in the event that the load balancing methods configured for this pool fail to return a valid virtual server. Use this option for A-type DNS queries. The default value is **::**.
- **fallback-ipv6**
  Specifies the IPv6 address of the server to which the system directs requests in the event that the load balancing methods configured for this pool fail to return a valid virtual server. Use this option for AAAA- and A6-type DNS queries. The default value is **::**.
- **fallback-mode**
  Specifies the load balancing mode that the system uses to load balance name resolution requests among the members of this pool, if the preferred and alternate modes are unsuccessful in picking a pool. You set the preferred mode using the **load-balancing-mode** option, and the alternate mode using the **alternate-mode** option. The default value is **return-to-dns**.
  The options are:
  - **completion-rate**
    Specifies that the Global Traffic Manager selects the virtual server that currently maintains the least number of dropped or timed-out packets during a transaction between a data center and the client LDNS.
  - **cpu**
    Specifies that the Global Traffic Manager selects the virtual server that currently has the most CPU processing time available to handle name resolution requests.

- **drop-packet**
  Specifies that the Global Traffic Manager does nothing with the packet, and simply drops the request.
- **fallback-ip**
  Specifies that the Global Traffic Manager returns the IP address that you specify as an answer to the query.
- **fewest-hops**
  Specifies that the Global Traffic Manager distributes connection requests to the virtual server in the data center that has the fewest router hops from the Local DNS.
- **global-availability**
  Specifies that the Global Traffic Manager distributes connection requests to virtual servers included in the pool in the order in which they are listed.
- **kilobytes-per-second**
  Specifies that the Global Traffic Manager distributes connection requests to the virtual server that is currently processing the fewest number of kilobytes per second.
- **least-connections**
  Specifies that the Global Traffic Manager distributes connection requests to the virtual server on the Local Traffic Manager that currently hosts the fewest connections.
- **lowest-round-trip-time**
  Specifies that the Global Traffic Manager distributes connection requests to the virtual server with the fastest measured round trip time between a data center and a client LDNS.
- **none**
  Specifies that there is no fallback mode. If the system cannot use the preferred or alternate load balancing modes, it uses the next pool to resolve the request. If there are no more pools available, the result is the same as when the value for the **fallback-mode** option is **return-to-dns**.
- **packet-rate**
  Specifies that the Global Traffic Manager assigns connection requests to the virtual server that is currently processing the fewest number of packets per second.
- **quality-of-service**
  Specifies that the Global Traffic Manager distributes connection requests using current performance information to calculate an overall score for each virtual server, and then distributes connections to the virtual servers based on these scores.
- **ratio**
  Specifies that the Global Traffic Manager distributes connection requests among a pool of virtual servers using a weighted Round Robin load balancing method.
- **return-to-dns**
  Specifies that the Global Traffic Manager immediately returns connection requests to the Local DNS for resolution.

- **round-robin**
  Specifies that the Global Traffic Manager distributes connection requests in a circular and sequential pattern among the virtual servers in a pool.
- **static-persistence**
  Specifies that the Global Traffic Manager consistently maps an LDNS IP address to the same available virtual server for the duration of a session.
- **topology**
  Specifies that the Global Traffic Manager uses proximity-based load balancing to distribute connection requests.
- **virtual-server-capacity**
  Specifies that the Global Traffic Manager distributes connection requests by creating a list of the virtual servers, weighted by capacity, then picks one of the virtual servers from the list. The virtual servers with the greatest capacity are picked most often, but over time all virtual servers are returned.
- **virtual-server-score**
  Specifies that the Global Traffic Manager assigns connection requests to virtual servers based on a user-defined ranking system.

◆ **glob**
Displays the items that match the **glob** expression. See **help glob** for a description of **glob** expression syntax.

◆ **limit-max-bps**
Specifies the maximum allowable data throughput rate, in bits per second, for the virtual servers in the pool. If the network traffic volume exceeds this value, the system marks the pool as unavailable. The default value is **0** (zero).

◆ **limit-max-bps-status**
Enables or disables the **limit-max-bps** option for this pool. The default value is **disabled**.

◆ **limit-max-connections**
Specifies the number of current connections allowed for the virtual servers in the pool. If the current connections exceed this value, the system marks the pool as unavailable. The default value is **0** (zero).

◆ **limit-max-connections-status**
Enables or disables the **limit-max-connections** option for this pool. The default value is **disabled**.

◆ **limit-max-pps**
Specifies the maximum allowable data transfer rate, in packets per second, for the virtual servers in the pool. If the network traffic volume exceeds this value, the system marks the pool as unavailable. The default value is **0** (zero).

◆ **limit-max-pps-status**
Enables or disables the **limit-max-pps** option for this pool. The default value is **disabled**.

- **load-balancing-mode**
  Specifies the preferred load balancing mode that the system uses to load balance name resolution requests among the members of this pool. The default value is **round-robin**.
  The options are:
  - **completion-rate**
    Specifies that the Global Traffic Manager selects the virtual server that currently maintains the least number of dropped or timed-out packets during a transaction between a data center and the client LDNS.
  - **cpu**
    Specifies that the Global Traffic Manager selects the virtual server that currently has the most CPU processing time available to handle name resolution requests.
  - **drop-packet**
    Specifies that the Global Traffic Manager does nothing with the packet, and simply drops the request.
  - **fallback-ip**
    Specifies that the Global Traffic Manager returns the IP address that you specify as an answer to the query.
  - **fewest-hops**
    Specifies that the Global Traffic Manager distributes connection requests to the virtual server in the data center that has the fewest router hops from the Local DNS.
  - **global-availability**
    Specifies that the Global Traffic Manager distributes connection requests to virtual servers included in the pool in the order in which they are listed.
  - **kilobytes-per-second**
    Specifies that the Global Traffic Manager distributes connection requests to the virtual server that is currently processing the fewest number of kilobytes per second.
  - **least-connections**
    Specifies that the Global Traffic Manager distributes connection requests to the virtual server on the Local Traffic Manager that currently hosts the fewest connections.
  - **lowest-round-trip-time**
    Specifies that the Global Traffic Manager distributes connection requests to the virtual server with the fastest measured round trip time between a data center and a client LDNS.
  - **packet-rate**
    Specifies that the Global Traffic Manager assigns connection requests to the virtual server that is currently processing the fewest number of packets per second.

- **quality-of-service**
  Specifies that the Global Traffic Manager distributes connection requests using current performance information to calculate an overall score for each virtual server, and then distributes connections to the virtual servers based on these scores.
- **ratio**
  Specifies that the Global Traffic Manager distributes connection requests among a pool of virtual servers using a weighted Round Robin load balancing method.
- **return-to-dns**
  Specifies that the Global Traffic Manager immediately returns connection requests to the Local DNS for resolution.
- **round-robin**
  Specifies that the Global Traffic Manager distributes connection requests in a circular and sequential pattern among the virtual servers in a pool.
- **static-persistence**
  Specifies that the Global Traffic Manager consistently maps an LDNS IP address to the same available virtual server for the duration of a session.
- **topology**
  Specifies that the Global Traffic Manager uses proximity-based load balancing to distribute connection requests.
- **virtual-server-capacity**
  Specifies that the Global Traffic Manager distributes connection requests by creating a list of the virtual servers, weighted by capacity, then picks one of the virtual servers from the list. The virtual servers with the greatest capacity are picked most often, but over time all virtual servers are returned.
- **virtual-server-score**
  Specifies that the Global Traffic Manager assigns connection requests to virtual servers based on a user-defined ranking system.

◆ **manual-resume**
Enables or disables the manual resume function for this pool. If you leave this option **disabled** (the default), then a member of this pool automatically becomes available for load balancing when its status changes from down to up. When the manual-resume option is **enabled**, if the status of a member of this pool changes from up to down, the pool member remains disabled indefinitely until you manually re-enable it.

◆ **max-address-returned**
Specifies the maximum number of available virtual servers that the system lists in an A record response. The default value is **1**.

◆ **members**
Specifies the vs-name of the pool members. The default value is **none**. You can also use the following options with pool members:

- **app-service**
  Specifies the name of the application service to which this pool member belongs. The default value is **none**. **Note:** If the

strict-updates option is **enabled** on the application service that owns the object, you cannot modify or delete this pool member. Only the application service can modify or delete this pool member.

- **depends-on**
  Specifies the name of the virtual server on which this pool member depends.
- **description**
  User defined description.
- **[enabled | disabled]**
  Specifies whether this pool member is available for load balancing. The default value is **enabled**.
- **limit-max-bps**
  Specifies the maximum allowable data throughput rate, in bits per second, for the pool member. If the network traffic volume exceeds this value, the system marks the pool member as unavailable.
- **limit-max-bps-status**
  Enables or disables the **limit-max-bps** option for this pool member. The default value is **disabled**.
- **limit-max-connections**
  Specifies the number of current connections allowed for this pool member. If the current connections exceed this value, the system marks this pool member as unavailable.
- **limit-max-connections-status**
  Enables or disables the **limit-max-connection** option for this pool member. The default value is **disabled**.
- **limit-max-pps**
  Specifies the maximum allowable data transfer rate, in packets per second, for this pool member. If the network traffic volume exceeds this value, the system marks this pool member as unavailable.
- **limit-max-pps-status**
  Enables or disables the **limit-max-pps** option for this pool member. The default value is **disabled**.
- **monitor**
  Enables or disables the monitor assigned to this pool member. The default value is **enabled**.
- **order**
  Specifies the order number of the pool member. The system uses this number with load balancing methods that involve prioritizing pool members, such as the Ratio load balancing method.
- **ratio**
  Specifies the weight of the pool member for load balancing purposes.
- **vs-name**
  Displays the name of the corresponding virtual server.

◆ **metadata**
Associates user defined data, each of which has name and value pair and persistence. Persistent(default) means the data will be saved into config file.

- **monitor**
  Specifies the health monitors that the system uses to determine whether it can use this pool for load balancing. The default value is **none**.
- **name**
  Specifies a unique name for the component. This option is required for the commands **create** and **modify**.
- **partition**
  Displays the partition within which the component resides.
- **qos-hit-ratio**
  Assigns a weight to the Hit Ratio performance factor for the Quality of Service dynamic load balancing mode. The default value is **5**.
- **qos-hops**
  Assigns a weight to the Hops performance factor when the value of the either the **load-balancing-mode** or **fallback-mode** options is quality-of-service. The default value is **0** (zero).
- **qos-kilobytes-second**
  Assigns a weight to the Kilobytes per Second performance factor when the value of the either the **load-balancing-mode** or **fallback-mode** options is quality-of-service. The default value is **3**.
- **qos-lcs**
  Assigns a weight to the Link Capacity performance factor when the value of the either the **load-balancing-mode** or **fallback-mode** options is quality-of-service. The default value is **30**.
- **qos-packet-rate**
  Assigns a weight to the Packet Rate performance factor when the value of the either the **load-balancing-mode** or **fallback-mode** options is quality-of-service. The default value is **1**.
- **qos-rtt**
  Assigns a weight to the Round Trip Time performance factor when the value of the either the **load-balancing-mode** or **fallback-mode** options is quality-of-service. The default value is **50**.
- **qos-topology**
  Assigns a weight to the Topology performance factor when the value of the either the **load-balancing-mode** or **fallback-mode** options is quality-of-service. The default value is **0** (zero).
- **qos-vs-capacity**
  Assigns a weight to the Virtual Server performance factor when the value of the either the **load-balancing-mode** or **fallback-mode** options is quality-of-service. The default value is **0** (zero).
- **qos-vs-score**
  Assigns a weight to the Virtual Server Score performance factor when the value of the either the **load-balancing-mode** or **fallback-mode** options is quality-of-service. The default value is **0** (zero).

- **regex**
  Displays the items that match the regular expression. The regular expression must be preceded by an at sign (@[regular expression]) to indicate that the identifier is a regular expression. See **help regex** for a description of regular expression syntax.
- **ttl**
  Specifies the number of seconds that the IP address, once found, is valid. Once the time-to-live (TTL) expires, the client has to request the IP address resolution again. The valid values are **0** through **4294967295**; the default value is **30**.
- **verify-member-availability**
  Specifies that the system verifies the availability of the members before sending a connection to those resources. The default value is **enabled**.

See Also

admin-partitions, *create*, *delete*, *edit*, glob, *gtm monitor*, *list*, *default-node-monitor*, *virtual*, *modify*, regex, *reset-stats*, *show*, *tmsh*

prober-pool

Configures prober pools for the Global Traffic Manager™.

Syntax

Modify the Global Traffic Manager **prober-pool** component within the **gtm** module using the syntax shown in the following sections.

Create/Modify

```
create prober-pool [name]
modify prober-pool [name]
  app-service [[string] | none]
  description [string]
  [disabled | enabled]
  load-balancing-mode [global-availability | round-robin]
  members none
  members
    [ add | delete | modify | replace-all-with ] {
      [name] {
          app-service [[string] | none]
          description [string]
          [disabled | enabled]
          order [integer]
     }...
  }
edit prober-pool [ [ [name] | [glob] | [regex] ] ... ]
  all-properties
  non-default-properties
reset-stats prober-pool
reset-stats prober-pool [ [ [name] | [glob] | [regex] ] ... ]
```

Display

```
list prober-pool
list prober-pool [ [ [name] | [glob] | [regex] ] ... ]
show running-config prober-pool
show running-config prober-pool [ [ [name] | [glob] | [regex] ] ... ]
  all-properties
  non-default-properties
show prober-pool
show prober-pool [name]
  (default | exa | gig | kil | meg | peta | raw | tera | yotta | zetta)
  detail
  field-fmt
```

Delete

```
delete prober-pool [name]
```

◆ Note

You must remove all references to a prober-pool before you can delete the prober-pool.

Description

You can use the prober-pool component to configure prober pool definitions on the Global Traffic Manager. You use prober pools to control which BIG-IP servers on your network are utilized by GTM to monitor the up/down state of GTM resources. Once defined, prober pools can be set to monitor whole data centers or individual servers.

Examples

create prober-pool my_pool members add {
bigip-dallas
bigip-london
}

Creates a Global Traffic Manager prober pool with two members **bigip-dallas** and **bigip-london**. Members are selected using the global-availability load balancing method.

delete prober-pool my_pool

Deletes the prober pool **my_pool**.

show prober-pool

Displays statistics for all prober pools.

list prober-pool my_pool

Displays settings of prober pool **my_pool**.

Options

- **app-service**
  Specifies the name of the application service to which this prober pool belongs. The default value is **none**. **Note:** If the **strict-updates** option is **enabled** on the application service that owns the object, you cannot modify or delete this prober pool. Only the application service can modify or delete this prober pool.
- **description**
  User defined description.

- **glob**
  Displays the items that match the **glob** expression. See **help glob** for a description of **glob** expression syntax.
- **load-balancing-mode**
  Specifies the load balancing mode that the system uses to select members of this pool. The default value is **global-availability**.
  The options are:
  - **global-availability**
    Specifies that the Global Traffic Manager selects the first available pool member in the order in which they are listed.
  - **round-robin**
    Specifies that the Global Traffic Manager selects members using a circular, sequential pattern among available pool members.
- **members**
  Specifies the BIG-IP server names of the pool members. The default value is **none**.
  You can also use the following options with prober pool members:
  - **app-service**
    Specifies the name of the application service to which this prober pool member belongs. The default value is **none**. **Note:** If the **strict-updates** option is **enabled** on the application service that owns the object, you cannot modify or delete this prober pool member. Only the application service can modify or delete this prober pool member.
  - **description**
    User defined description.
  - **[enabled | disabled]**
    Specifies whether this pool member is available to issue probes. The default value is **enabled**.
  - **order**
    Specifies the order number of the pool member. The system uses this number with load balancing methods that involve prioritizing pool members by listed order.
- **name**
  Specifies a unique name for the component. This option is required for the commands **create**, **delete**, and **modify**.
- **regex**
  Displays the items that match the regular expression. The regular expression must be preceded by an at sign (@[regular expression]) to indicate that the identifier is a regular expression. See **help regex** for a description of regular expression syntax.

See Also

create, *delete*, *edit*, glob, *server*, *datacenter*, *list*, *modify*, regex, *reset-stats*, *show*, *tmsh*

region

Configures a Global Traffic Manager™ region.

Syntax

Configure the **region** component within the **gtm** module using the syntax shown in the following sections.

Create/Modify

```
create region [name]
modify region [name]
  app-service [[string] | none]
  description [string]
  [name]
  region-members
    app-service [[string] | none]
    continent [Africa | Antarctica | Asia | Australia | Europe
        | North America | South America | unknown]
    country [two-letter abbreviation of country name]
    datacenter [name]
    isp [AOL | BeijingCNC | CNC | ChinaTelecom | Comcast | Earthlink
        | ShanghaiCNC | ShanghaiTelecom]
    not [continent | country | datacenter | isp | pool | region-name
        | subnet]
    pool [name]
    region-name [name]
    state [name]
    subnet
edit region [ [ [name] | [glob] | [regex] ] ... ]
  all-properties
```

Display

```
list region
list region [ [ [name] | [glob] | [regex] ] ... ]
show running-config region
show running-config region [ [ [name] | [glob] | [regex] ] ... ]
    all-properties
    one-line
```

Delete

```
delete region [name]
```

Description

You can use the **region** component to create, display, modify, or delete a region. A region is a customized collection of topologies with which you can extend the topology functionality by defining specific geographical regions that have meaning for your network.

Examples

create region my_region continent Australia

Creates a region named **my_region** to populate with resources on the continent of Australia.

list region

Displays properties for all regions.

delete region my_region

Deletes the region named **my_region**.

Options

- **app-service**
  Specifies the name of the application service to which the region belongs. The default value is **none**. **Note:** If the **strict-updates** option is **enabled** on the application service that owns the object, you cannot modify or delete the region. Only the application service can modify or delete the region.
- **description**
  User defined description.
- **glob**
  Displays the items that match the **glob** expression. See **help glob** for a description of **glob** expression syntax.
- **name**
  Specifies a unique name for the component. This option is required for the commands **create** and **modify**.
- **regex**
  Displays the items that match the regular expression. The regular expression must be preceded by an at sign (@[regular expression]) to indicate that the identifier is a regular expression. See **help regex** for a description of regular expression syntax.
- **region-members**
  Specifies the members that you want to add to, delete from, replace-all-with, or modify for this region.
  You can specify the following options for region members:
  - **app-service**
    Specifies the name of the application service to which the region member belongs. The default value is **none**. **Note:** If the **strict-updates** option is **enabled** on the application service that owns the object, you cannot modify or delete the region member. Only the application service can modify or delete the region member.
  - **continent**
    Specifies the name of a continent.
  - **country**
    Specifies the two-letter abbreviation of a country. Use the command completion feature to view the numerous options.

- **datacenter**
  Specifies the name of an existing data center.
- **isp**
  Specifies the name of an Internet service provider.
- **not**
  Specifies region-members to exclude from this region.
- **pool**
  Specifies the name of an existing pool.
- **region-name**
  Specifies the name of an existing region.
- **state**
  Specifies the name of an existing state.
- **subnet**
  Specifies an existing subnet.

See Also

create, *delete*, *edit*, glob, *list*, *modify*, regex, *show*, *tmsh*

rule

Opens an editor in which you can configure iRules® for traffic management system configuration.

Syntax

Configure the **rule** component within the **gtm** module using the syntax shown in the following sections.

Create/Modify

```
create rule [name]
modify rule [name]
  option:
    metadata
      [add | delete | modify] {
        [metadata_name] {
          value [ "value content" ]
          persist [ true | false ]
          }
    }
edit rule [ [ [name] | [glob] | [regex] ] ... ]
```

Display

```
list rule
list rule [ [ [name] | [glob] | [regex] ] ... ]
show running-config rule
show running-config rule [ [ [name] | [glob] | [regex] ] ... ]
    all-properties
    non-default-properties
show rule
show rule [ [ [name] | [glob] | [regex] ] ... ]
    (default | exa | gig | kil | meg | peta | raw | tera | yotta | zetta)
    field-fmt
```

Delete

```
delete rule [name]
```

◆ Note

You can also delete metadata associated with an iRule. See the example section for detail.

Description

You can use iRules to direct traffic not only to specific pools, but also to individual pool members, including port numbers and URI paths, either to implement persistence or to meet specific load balancing requirements. The syntax that you use to write iRules is based on the Tools Command

Language (TcL) programming standard. Thus, you can use many of the standard TcL commands, plus a robust set of extensions that the BIG-IP® local traffic management system provides to help you further increase load balancing efficiency.

For information about standard TcL syntax, see **http://tmml.sourceforge.net/doc/tcl/index.html**. For a list of TcL commands that have been disabled within the traffic management system and therefore cannot be used in the traffic management system, see the *Configuration Guide for BIG-IP® Local Traffic Management®*. This guide is available at **https://support.f5.com**.

Examples

edit rule my_irule

Opens the **vi** editor in which you can edit the iRule named **my_irule**. Note that after you close the editor, you must run the command sequence **save config** to save the configuration changes to the stored configuration files.

The following are example iRules for the Global Traffic Manager™.

```
when DNS_REQUEST {
   if {[IP::addr [IP::remote_addr]/24 equals 10.10.1.0/24] }
      {cname cname.siterequest.com } else { host 10.20.20.20}}
```

Specifies that requests from **10.10.1.0/24** be directed to **cname.siterequest.com**, and all other requests be directed to **10.20.20.20**.

```
when DNS_REQUEST {
   if {[whereis [IP::remote_addr]] contains "Asia"}
      {pool asia_pool} else {pool general_pool}}
```

Specifies that requests that originate in Asia be directed to the pool named **asia_pool**, and that all other requests be directed to the pool named **general_pool**.

metadata is the user defined key/value pair

Adds new metadata to named **my_meta** and modifies existing metadata named **my_meta2** for the iRule named **my_irule**.

```
modify rule my_irule {
   when DNS_REQUEST {}
   metadata replace-all-with {
   my_meta {
persist false
value "hello"
}
      my_meta2 {
persist false
value "hello 2"
}
   }
}
```

Deletes metadata named **my_meta** from the iRule named **my_irule**.

```
modify rule my_irule {
   when RULE_INIT {}
   definition-checksum 7c0dba9aa53e8959042c6cfe041d3d11
   metadata delete { my_meta }
}
```

Options

- **glob**
  Displays the items that match the **glob** expression. See **help glob** for a description of **glob** expression syntax.
- **metadata**
  Specifies a user-defined key/value pair.
- **name**
  Specifies a unique name for the component. This option is required.
- **regex**
  Displays the items that match the regular expression. The regular expression must be preceded by an at sign (@[regular expression]) to indicate that the identifier is a regular expression. See **help regex** for a description of regular expression syntax.

See Also

edit, glob, *list*, regex, *show*, *tmsh*

server

Configures servers for the Global Traffic Manager™.

Syntax

Configure the **server** component within the **gtm** module using the syntax shown in the following sections.

Create/Modify

```
create server [name]
modify server [name]
  addresses none
  addresses
    [add | delete | replace-all-with] {
      [ip address] {
          app-service [[string] | none]
          device-name [none | [name] ]
          translation [ip address]
          explicit-link-name [none | [name] ]
      }
  }
  app-service [[string] | none]
  datacenter
  datacenter [name]
  description [string]
  [disabled | enabled]
  expose-route-domains [no | yes]
  iq-allow-path [no | yes]
  iq-allow-service-check [no | yes]
  iq-allow-snmp [no | yes]
  limit-cpu-usage [integer]
  limit-cpu-usage-status [disabled | enabled]
  limit-mem-avail [integer]
  limit-mem-avail-status [disabled | enabled]
  limit-max-bps [integer]
  limit-max-bps-status [disabled | enabled]
  limit-max-connections [integer]
  limit-max-connections-status [disabled | enabled]
  limit-max-pps [integer]
  limit-max-pps-status [disabled | enabled]
  link-discovery [disabled | enabled]
  metadata
    [add | delete | modify] {
      [metadata_name ... ] {
        value [ "value content" ]
        persist [ true | false ]
      }
  }
  monitor [none | [name] ]
  prober-pool [none | name]
  product [name]
  virtual-server-discovery [disabled | enabled]
  virtual-servers none
  virtual-servers
    [add | delete | replace-all-with] {
```

```
        [vs-name] {
            app-service [[string] | none]
            depends-on none
            depends-on
              [add | delete | replace-all-with] {
                [server_name:vs-name]...
            }
            description [string]
            destination [ipv4_address:port | ipv6_address.port]
            [disabled | enabled]
            explicit-link-name [none | [name] ]
            limit-max-bps [integer]
            limit-max-bps-status [disabled | enabled]
            limit-max-connections [integer]
            limit-max-connections-status [disabled | enabled]
            limit-max-pps [integer]
            limit-max-pps-status [disabled | enabled]
            ltm-name [name]
            monitor [name]
            translation-address [ip address]
            translation-port [ [integer] | [name] ]
        }
    }
edit server [ [ [name] | [glob] | [regex] ] ... ]
    all-properties
    non-default-properties
    one-line
reset-stats server
reset-stats server [ [ [name] | [glob] | [regex] ] ... ]
```

Display

```
list server
list server [ [ [name] | [glob] | [regex] ] ... ]
show running-config server
show running-config server [ [ [name] | [glob] | [regex] ] ... ]
    all-properties
    non-default-properties
    partition
show server
show server [ [ [name] | [glob] | [regex] ] ... ]
    (default | exa | gig | kil | meg | peta | raw | tera | yotta | zetta)
    detail
    field-fmt
```

Delete

```
delete server [name]
```

Description

You can use the server component to configure a Global Traffic Manager server.

Examples

create server my_server addresses add {10.10.1.1} datacenter my_datacenter

Creates a server named **my_server** in **my_datacenter** with a self IP address of **10.10.1.1**.

modify server my_server virtual-servers add {myVs { address 10.10.10.2:80 } }

Adds the virtual server myVs with an IP address of **10.10.10.2:80** as a resource to the server named **my_server**.

list server non-default-properties

Displays all non-default properties for all servers.

delete server my_server

Deletes the server named **my_server**.

show server *my_server* **detail**

Shows the link associated with each server IP address for *my_server*.

show server all detail

Shows the link assignments for all servers in the system.

show server *my_server* **virtual-servers**

Shows the regular server information as well as any virtuals on *my_server*. The link associated with a virtual server is displayed, or --- is shown to indicate that the virtual is not using a configured link.

Options

- **addresses**
  Specifies the server IP addresses for the server. This option is required for the command **create**. You can also specify the following options:
  - **app-service**
    Specifies the name of the application service to which the self IP address belongs. The default value is **none**. **Note:** If the **strict-updates** option is **enabled** on the application service that owns the object, you cannot modify or delete the self IP address. Only the application service can modify or delete the self IP address.
  - **device-name**
    Specifies the name of this system in a redundant pair. The default value is the server name.
  - **explicit-link-name**
    Specifies the explicit link name for the server. The default value is **none**.
  - **translation**
    Specifies the internal IP address that corresponds to the external IP address of this server. The default value is **::**.

- **app-service**
  Specifies the name of the application service to which the server belongs. The default value is **none**. **Note:** If the **strict-updates** option is **enabled** on the application service that owns the object, you cannot modify or delete the server. Only the application service can modify or delete the server.
- **datacenter**
  Specifies the data center to which the server belongs. This option is required for the command **create**.
- **description**
  User defined description.
- **detail**
  The **detail** option is used with the **show** display command. This shows the link associated with each server IP address. Only the server IP addresses that have an associated link are displayed. If this server is not using any links, no link assignment information is printed. By default, links are automatically matched to server IP addresses according to their IP addresses. Explicit links may also be defined. How this link was assigned is displayed in the Link Assignment column: **auto** means that the system automatically assigned this link, and **explicit** means that the link was explicitly set by the user.
- **[disabled | enabled]**
  Enables or disables the server. The default value is **enabled**.
- **expose-route-domains**
  Allow the GTM server to auto-discover LTM virtual servers from all route domains. The default value is **no**.
- **glob**
  Displays the items that match the **glob** expression. See **help glob** for a description of **glob** expression syntax.
- **iq-allow-path**
  Specifies whether the Global Traffic Manager uses this BIG-IP® system to conduct a path probe before delegating traffic to it. The default value is **yes**.
- **iq-allow-service-check**
  Specifies whether the Global Traffic Manager uses this BIG-IP system to conduct a service check probe before delegating traffic to it. The default value is **yes**.
- **iq-allow-snmp**
  Specifies whether the Global Traffic Manager uses this BIG-IP system to conduct an SNMP probe before delegating traffic to it. The default value is **yes**.
- **limit-cpu-usage**
  For a server configured as a generic host, specifies the percent of CPU usage, otherwise has no effect. If percent of CPU usage goes above the limit, the system marks the server as unavailable.

- **limit-cpu-usage-status**
  Enables or disables the **limit-cpu-usage** option for this server. Only has an effect on a server configured as a generic host. The default value is **disabled**.
- **limit-mem-avail**
  For a server configured as a generic host, specifies the available memory required by the virtual servers on the server. If available memory falls below this limit, the system marks the server as unavailable.
- **limit-mem-avail-status**
  Enables or disables the **limit-mem-avail** option for this server. Only used on a server configured as a generic host. The default value is **disabled**.
- **limit-max-bps**
  Specifies the maximum allowable data throughput rate, in bits per second, for this server. If the network traffic volume exceeds this limit, the system marks the server as unavailable.
- **limit-max-bps-status**
  Enables or disables the **limit-max-bps** option for this server. The default value is **disabled**.
- **limit-max-connections**
  Specifies the maximum number of concurrent connections, combined, for this server. If the connections exceed this limit, the system marks the server as unavailable.
- **limit-max-connections-status**
  Enables or disables the **limit-max-connections** option for this server. The default value is **disabled**.
- **limit-max-pps**
  Specifies the maximum allowable data transfer rate, in packets per second, for this server. If the network traffic volume exceeds this limit, the system marks the server as unavailable.
- **limit-max-pps-status**
  Enables or disables the **limit-max-pps** option for this server. The default value is **disabled**.
- **link-discovery**
  Specifies whether the system auto-discovers the links for this server. The default value is **disabled**. The options are:
  - **disabled**
    Specifies that the system does not auto-discover the links that are available for the server.
  - **enabled**
    Specifies that the system auto-discovers the links that are configured on the server. With this option, the system automatically adds, deletes, and modifies link settings in the configuration.
  - **enabled-no-delete**
    Specifies that the system auto-discovers the links that are configured on the server. With this option, the system automatically adds and

modifies link settings in the configuration, but does not delete them. This option is useful when you regularly take links in and out of service.

- **monitor**
  Specifies the health monitors that the system uses to determine whether this server is available for load balancing.
- **metadata**
  Specifies user-defined data to associate with a server. By default the **persist attribute** is set to **true**. This means the data is saved into the configuration file.
- **name**
  Specifies a unique name for the component. This option is required for the commands **create** and **modify**.
- **partition**
  Displays the administrative partition within which the object resides.
- **prober-pool**
  Specifies the name of a prober pool to use to monitor this server's resources. If this value is specified, it overrides any prober pool set on this server's data center. The default value is **none**.
- **product**
  Specifies the server type. The server type determines the metrics that the system can collect from the server. Use the command completion feature to view the types of servers that are available.
- **regex**
  Displays the items that match the regular expression. The regular expression must be preceded by an at sign (@[regular expression]) to indicate that the identifier is a regular expression. See **help regex** for a description of regular expression syntax.
- **virtual-server-discovery**
  Specifies whether the system auto-discovers the virtual servers for this server. The default value is **disabled**. The options are:
  - **disabled**
    Specifies that the system does not auto-discover the virtual servers that are configured on the server. With this option, you must configure the virtual servers for this server.
  - **enabled**
    Specifies that the system auto-discovers the virtual servers that are configured on the server. With this option, the system automatically adds, deletes, and modifies virtual server settings in the configuration.
  - **enabled-no-delete**
    Specifies that the system auto-discovers the virtual servers that are configured on the server. With this option, the system automatically adds and modifies virtual server settings in the configuration, but does not delete them. This option is useful when you regularly take virtual servers in and out of service.

- **virtual-servers**
  Specifies the name of the virtual servers that are resources for this server. You can include the following options for virtual servers.
  - **app-service**
    Specifies the name of the application service to which the virtual server belongs. The default value is **none**. **Note:** If the **strict-updates** option is **enabled** on the application service that owns the object, you cannot modify or delete the virtual server. Only the application service can modify or delete the virtual server.
  - **depends-on**
    Specifies the vs-name of the server on which this virtual server depends.
  - **description**
    User defined description.
  - **destination**
    Specifies the IP address and port of the virtual server.
  - **[disabled | enabled]**
    Specifies whether this virtual server is available for load balancing. The default value is **enabled**.
  - **explicit-link-name**
    Specifies the explicit link name for the virtual server. The default value is **none**.
  - **limit-max-bps**
    Specifies the maximum allowable data throughput rate, in bits per second, for this virtual server. If the network traffic volume exceeds this value, the system marks the virtual server as unavailable. The default value is **0** (zero).
  - **limit-max-bps-status**
    Enables or disables the **limit-max-bps** option for this virtual server. The default value is **disabled**.
  - **limit-max-connections**
    Specifies the number of current connections allowed for this virtual server. If the current connections exceed this value, the system marks this virtual server as unavailable. The default value is **0** (zero).
  - **limit-max-connections-status**
    Enables or disables the **limit-max-connections** option for this virtual server. The default value is **disabled**.
  - **limit-max-pps**
    Specifies the maximum allowable data transfer rate, in packets per second, for this virtual server. If the network traffic volume exceeds this limit, the system marks the virtual server as unavailable. The default value is **0** (zero).
  - **limit-max-pps-status**
    Enables or disables the **limit-max-pps** option for this virtual server. The default value is **disabled**.

- **ltm-name**
  The virtual server name found on the LTM. Useful for differentiating between virtuals with same IP and port, but different protocols. The **ltm-name** used in probe requests.
- **monitor**
  Specifies the monitor you want to assign to this virtual server. The default value is **none**.
- **translation-address**
  Specifies the public address that this virtual server translates into when the Global Traffic Manager communicates between the network and the Internet. The default value is **::**.
- **translation-port**
  Specifies the translation port number or service name for the virtual server, if necessary. The default value is **0**.

See Also

create, *delete*, *edit*, glob, *datacenter*, *link*, *prober-pool*, *list*, *modify*, regex, *reset-stats*, *show*, *tmsh*

topology

Configures a topology statement.

Syntax

Configure the **topology** component within the **gtm** module using the syntax shown in the following sections.

Create

```
create topology
    app-service [[string] | none]
    description [string]
    ldns: [continent | country | isp | not | region-name | state | subnet]
    server: [continent | country | datacenter | isp | not | pool |
             region-name | state | subnet]
    score [integer]
edit topology [ [name] | [glob] | [regex] ] ... ]
    all-properties
    non-default-properties
```

Display

```
list topology
list topology [ [name] | [glob] | [regex] ] ... ]
show running-config topology
show running-config topology [ [name] | [glob] | [regex] ] ... ]
    all-properties
    non-default-properties
    one-line
```

Delete

```
delete topology all
delete topology
  [ldns: [identifier] [value] server: [identifier] [value] ]
```

Description

You can use the **topology** component to configure a topology statement. A topology statement is a set of characteristics that identify the origin of a given name resolution request.

Examples

create topology ldns: country US server: datacenter DC1 score 30

Creates a topology statement that specifies that the Global Traffic Manager routes any traffic coming from the United States to the datacenter named **DC1**. Note that the weight of this topology item for load balancing is **30**.

delete topology ldns: country US server: datacenter DC1

Deletes the topology statement mentioned in the previous example.

Options

- **app-service**
  Specifies the name of the application service to which the topology belongs. The default value is **none**. **Note:** If the **strict-updates** option is **enabled** on the application service that owns the object, you cannot modify or delete the topology. Only the application service can modify or delete the topology.
- **description**
  User defined description.
- **glob**
  Displays the items that match the **glob** expression. See **help glob** for a description of **glob** expression syntax.
- **ldns:**
  Specifies the criteria that the Global Traffic Manager uses when matching requests from LDNS servers.
  - **continent**
    A continent whose IP address allocation range should be used in matching topologies
  - **country**
    A country whose IP address allocation range should be used in matching topologies
  - **datacenter**
    A data center to be used in matching topologies
  - **isp**
    An ISP whose IP address allocation range should be used in matching topologies
  - **not**
    Specify a region member to exclude from the region
  - **pool**
    A pool to be used in matching topologies
  - **region**
    Another region to be used in matching topologies
  - **state**
    A state whose IP address allocation range should be used in matching topologies
  - **subnet**
    A subnet to be used in matching topologies

- **regex**
  Displays the items that match the regular expression. The regular expression must be preceded by an at sign (@[regular expression]) to indicate that the identifier is a regular expression. See **help regex** for a description of regular expression syntax.
- **score**
  Specifies the weight of the topology item.
- **server:**
  Specifies the server to which the Global Traffic Manager routes requests.
  - **continent**
    A continent whose IP address allocation range should be used as an LDNS routing destination
  - **country**
    A country whose IP address allocation range should be used as an LDNS routing destination
  - **datacenter**
    A data center to be used as an LDNS routing destination
  - **isp**
    An ISP whose IP address allocation range should be used as an LDNS routing destination
  - **not**
    Specify an item to exclude from the group
  - **pool**
    A pool to be used as an LDNS routing destination
  - **region**
    Another region to be used as an LDNS routing destination
  - **state**
    A state whose IP address allocation range be used as an LDNS routing destination
  - **subnet**
    A subnet to be used as an LDNS routing destination

See Also

create, *delete*, *edit*, glob, *server*, *list*, regex, *show*, *tmsh*,

traffic

Displays traffic statistics for the Global Traffic Manager™.

Syntax

Configure the **traffic** component within the **gtm** module using the syntax in the following section.

Display

```
show traffic
    (default | exa | gig | kil | meg | peta | raw | tera | yotta | zetta)
    field-fmt
```

Description

You can use the **traffic** component to display traffic statistics, including those for IPv4 and IPv6 requests, current Local Domain Name System (LDNS) servers, and current paths.

See Also

show, *tmm-traffic*, *tmsh*

wideip

Configures a wide IP.

Syntax

Configure the **wideip** component within the **gtm** module using the syntax shown in the following sections.

Create/Modify

```
create wideip [name]
modify wideip [name]
    aliases [name...name]
    app-service [[string] | none]
    description [string]
    [disabled | enabled]
    ipv6-no-error-neg-ttl [integer]
    ipv6-no-error-response [disabled | enabled]
    last-resort-pool [name]
    load-balancing-decision-log-verbosity [[pool-selection | pool-traversal |
pool-member-selection | pool-member-traversal] | none]
    metadata
      [add | delete | modify] {
        [metadata_name ... ] {
          value [ "value content" ]
          persist [ true | false ]
        }
    }
 persistence [disabled | enabled]
    persist-cidr-ipv4 [integer]
    persist-cidr-ipv6 [integer]
    pool-lb-mode [name]
    pools none
    pools
      [add | delete | modify | replace-all-with] {
        [pool name]...
    }
    rules none
    rules
      [add | delete | modify | replace-all-with] {
          [rule name]...
    }
    ttl-persistence [integer]
edit wideip [ [name] | [glob] | [regex] ] ... ]
    all-properties
    non-default-properties
reset-stats wideip
reset-stats wideip [ [name] | [glob] | [regex] ] ... ]
```

Display

```
list wideip
list wideip [ [name] | [glob] | [regex] ] ... ]
show running-config wideip
show running-config wideip [ [name] | [glob] | [regex] ] ... ]
```

```
    all-properties
    non-default-properties
    one-line
    partition
show wideip
show wideip [ [ [name] | [glob] | [regex] ] ... ]
    (default | exa | gig | kil | meg | peta | raw | tera | yotta | zetta)
    (detail | global)
    field-fmt
```

Delete

```
delete wideip [all | [name] ]
```

Description

You can use the **wideip** component to create, modify, display, or delete a wide IP. A wide IP is a mapping of a fully-qualified domain name (FQDN) to a set of virtual servers that host the domain's content, such as a web site or an e-commerce site.

Examples

create wideip www.my_wide_ip.com

Creates a wide IP named **www.my_wide_ip.com**.

delete wideip www.my_wide_ip.com

Deletes the wide IP named **www.my_wide_ip**.

Options

- **aliases**
  Specifies alternate domain names for the web site content you are load balancing. You can use two different wildcard characters, asterisk (*) and question mark (?), to represent one or more characters. The default value is **none**.
- **app-service**
  Specifies the name of the application service to which this wide ip belongs. The default value is **none**. **Note:** If the **strict-updates** option is **enabled** on the application service that owns the object, you cannot modify or delete this wide ip. Only the application service can modify or delete this wide ip.
- **description**
  User defined description.
- **[disabled | enabled]**
  Specifies whether the wide IP and its resources are available for load balancing.

- **glob**
  Displays the items that match the **glob** expression. See **help glob** for a description of **glob** expression syntax.
- **ipv6-no-error-neg-ttl**
  Specifies the negative caching TTL of the SOA for the IPv6 NoError response. The default is 0, meaning no SOA is included (i.e. no caching).
- **ipv6-no-error-response**
  When **enabled**, specifies that the system returns a NoError response to IPv6 wide IP requests. This response is an authoritative empty answer from the system to AAAA record requests. With this option **enabled**, the system responds faster to IPv6 requests for which it does not have AAAA records configured. The default value is **disabled**.
- **last-resort-pool**
  Specifies which pool for the system to use as the last resort pool when load balancing requests for this wide IP. The default value is **none**.
- **load-balancing-decision-log-verbosity**
  Specifies the amount of detail logged when making load balancing decisions. This is used for debugging purpose only. Performance will be affected if the value is not **none**. Please reset it back to **none** after done debugging. With the option **pool-selection**, the log will contain pool load balancing algorithm details. This includes common actions taken to a set of pools (for example, whether all pools reset the ratio counter during the algorithm) and the result of the load balancing algorithm (for example, whether a pool is finally selected and the reason if applicable). With the option **pool-traversal**, the log will contain details of all pools traversed during load balancing. With the option **pool-member-selection**, the log will contain pool member load balancing algorithm details. This includes common actions taken to a set of pool members and the result of the load balancing algorithm. With the option **pool-member-traveral**, the log will contain details of all pool members traversed during load balancing. The default value is **none**.
- **metadata**
  Specifies user-defined data to associate with a server. By default the **persist** attribute is set to true. This means the data is saved into the configuration file.
- **name**
  Specifies a unique name for the component. This option is required for the commands **create** and **modify**.
- **partition**
  Displays the administrative partition within which the component resides.
- **persistence**
  When **enabled**, specifies that when a local DNS server makes repetitive requests on behalf of a client, the system reconnects the client to the same resource as previous requests. The default value is **disabled**.

- **persist-cidr-ipv4**
  Specifies a mask used to group IPv4 LDNS addresses. This feature allows one persistence record to be shared by LDNS addresses that match within this mask.
- **persist-cidr-ipv6**
  Specifies a mask used to group IPv6 LDNS addresses. This feature allows one persistence record to be shared by LDNS addresses that match within this mask.
- **pools**
  Configures the pools the system uses when load balancing requests for this wide IP. The default value is **none**.
- **pool-lb-mode**
  Specifies the load balancing method used to select a pool in this wide IP. This option is relevant only when multiple pools are configured for this wide IP. The default value is **round-robin**.
  The available load balancing methods are:
  - **global-availability**
    Specifies that the system selects a pool by following the order of the Pool list. The system repeatedly selects the first pool in the list for as long as its status is available. If the pool becomes unavailable for any reason, the system then repeatedly selects the next pool in the list, and so on.
  - **random**
    Specifies that the system selects a pool in no pattern or order.
  - **ratio**
    Specifies that the system selects a pool based on the ratio that you assign to the pool.
  - **round-robin**
    Specifies that the system selects pools sequentially.
  - **topology**
    Specifies that the system selects a pool based on topology information in the incoming LDNS request. Note that this load balancing method works only if you have configured a topology statement.
- **regex**
  Displays the items that match the regular expression. The regular expression must be preceded by an at sign (@[regular expression]) to indicate that the identifier is a regular expression. See **help regex** for a description of regular expression syntax.
- **rules**
  Specifies the iRules® that this wide IP uses for load balancing decisions. The system evaluates the iRules in the order in which they are listed, until it finds a matching iRule. The default value is **none**.
- **ttl-persistence**
  Specifies, in seconds, the length of time for which a persistence entry is valid. This value can range from **0** through **4294967295** seconds. The default value is **3600**.

See Also

create, *delete*, *edit*, glob, *pool*, *list*, *modify*, regex, *reset-stats*, *show*, *tmsh*

47

gtm global-settings

- Introducing the gtm global-settings module
- Alphabetical list of components

Introducing the gtm global-settings module

You can use the tmsh components that reside within the gtm global-settings module to configure general, load balancing, and metrics settings for the Global Traffic Manager™. You can also configure the metrics address exclusions list. For more information about the tmsh hierarchical structure, see Chapter 2, *Understanding and Using the Traffic Management Shell*.

Alphabetical list of components

The remainder of this chapter lists the tmsh components that are available in the gtm global-settings module.

general

Configures the general settings for the Global Traffic Manager.

Syntax

Modify or display the **general** component within the **gtm global-settings** module using the syntax in the following sections.

Modify

```
modify general
    automatic-configuration-save-timeout [integer]
    auto-discovery [no | yes]
    auto-discovery-interval [integer]
    cache-ldns-servers [no | yes]
    domain-name-check [allow-underscore | idn-compatible | none
        | strict]
    drain-persistent-requests [no | yes]
    forward-status [enable | disable]
    gtm-sets-recursion [no | yes]
    heartbeat-interval [integer]
    montior-disabled-objects [no | yes]
    nethsm-timeout [integer]
    peer-leader [name]
    send-wildcard-rrs [enable | disable]
    static-persist-cidr-ipv4 [integer]
    static-persist-cidr-ipv6 [integer]
    synchronization [no | yes]
    synchronization-group-name [name]
    synchronization-time-tolerance [integer]
    synchronization-timeout [integer]
    synchronize-zone-files [no | yes]
    synchronize-zone-files-timeout [integer]
    topology-allow-zero-scores [no | yes]
    virtuals-depend-on-server-state [no | yes]
edit general
   all-properties
   non-default-properties
   one-line
```

Display

```
list
list general
show running-config general
show running-config general [option name]
    all-properties
    non-default-properties
```

Description

You can use the **general** component to modify or display the General Traffic Manager settings.

Examples

modify general auto-discovery no

Turns off auto-discovery for the Global Traffic Manager.

list general all-properties

Displays all properties of the general settings for the Global Traffic Manager.

Options

- **automatic-configuration-save-timeout**
  Sets the timeout, in seconds, indicating how long to wait after a GTM configuration change before automatically saving the GTM configuration to the bigip_gtm.conf. A timeout of -1 will cause the GTM configuration to NEVER be saved. A value of 0 will cause the GTM configuration to be saved immediately. The default value is **15** seconds.
- **auto-discovery**
  Specifies whether the auto-discovery process is activated for this system. The default value is **no**.
- **auto-discovery-interval**
  Specifies the frequency, in seconds, between system attempts to discover network components. The default value is **30**.
- **cache-ldns-servers**
  Specifies whether the system retains, in cache, all local DNS servers that make requests. The default value is **yes**.
  You must enable this option if you want the system to store and use the LDNS path information.
- **domain-name-check**
  Specifies the parameters for the Global Traffic Manager to use when performing domain name checking. The default value is **strict**.
  The possible values are:
  - **allow-underscore**
    Underscores are allowed in domain names.
  - **idn-compatible**
    International domain names are allowed.
  - **none**
    Domain names are not allowed.
  - **strict**
    The Global Traffic Manager checks domain names according to the specifications in RFC 1123 Requirements for Internet Hosts - Application and Support.
- **drain-persistent-requests**
  Specifies, when set to **yes**, that when you disable a pool, load-balanced, persistent connections remain connected until the TTL expires. The default value is **yes**. If you set this option to **no**, any persistent connections terminate immediately when a pool is disabled.

- **forward-status**Specifies, when set to **enabled**, that the availibility status change for GTM objects will be shared with subscribers. This option will enable iControl clients to receive event notifications when a change occurs.

- **gtm-sets-recursion**
  Specifies, when set to **yes**, that the system enables recursive DNS queries, regardless of whether the requesting local DNS enabled recursive queries. The default value is **no**.
- **heartbeat-interval**
  Specifies the frequency at which the Global Traffic Manager queries other BIG-IP® systems for updated data. When configuring monitors for BIG-IP systems, F5 Networks recommends that the **probe-interval** option for the monitor be equal to or greater than the this option. The default value is **10**.
- **monitor-disabled-objects**
  Specifies, when set to **yes**, that the system will continue to monitor objects even if the objects are disabled. The default value is **no**.
- **nethsm-timeout**
  Time to wait on a NetHSM key creation operation for DNSSEC before retry. Default is **20** seconds.
- **peer-leader**
  Specifies the name of a GTM server to be used for executing certain features, such as creating DNSSEC keys.
- **send-wildcard-rrs**
  Specifies, when set to **enable**, that WideIPs or WideIP aliases that contain wildcards will autogenerate Resource Records in the BIND database. The default value is **disable**.
- **static-persist-cidr-ipv4**
  Specifies the number of bits of the IPv4 address that the system considers when using the Static Persist load balancing mode. The default value is **32**.
- **static-persist-cidr-ipv46**
  Specifies the number of bits of the IPv6 address that the system considers when using the Static Persist load balancing mode. The default value is **128**.
- **synchronization**
  Specifies whether this system is a member of a synchronization group. The default value is **no**.
  Members of the synchronization group continuously share configuration and metrics collection information. The synchronization group can contain Global Traffic Managers and Link Controllers.
- **synchronization-group-name**
  Specifies the name of the synchronization group to which the system belongs. The default name is **default**.
- **synchronization-time-tolerance**
  Specifies the number of seconds that one system clock can be out of sync with another system clock, in the synchronization group. If the variance

between the clock times is higher than the value of this option, the system resets the clock that is running behind to match the clock with the most recent time.
Possible values are **0** (zero), and **5** - **600**. (Values 1 through 4 are automatically set to 5, and 0 (zero) turns time synchronization off.) The default value is **10** seconds.

◆ Note

If you are using NTP to synchronize the clock with a time server, select a time tolerance other than 0 (zero). When you do this, the system uses the ***synchronization-time-tolerance*** *option as a fail-over mechanism if NTP is disabled for any reason.*

- **synchronization-timeout**
  Specifies the number of seconds that the system attempts to synchronize the Global Traffic Manager configuration with a synchronization group member. If the synchronization times out, the system tries again. The default value is **180**.
- **synchronize-zone-files**
  Specifies whether the system synchronizes zone files among the synchronization group members. The default value is **no**.
- **synchronize-zone-files-timeout**
  Specifies the number of seconds that a synchronization group member attempts to synchronize its zone files with a synchronization group member. If the synchronization times out, the system tries again. The default value is **300**.
- **topology-allow-zero-scores**
  Specifies if topology load-balancing or QoS load-balancing with topology enabled will return pool members with zero topology scores. The default value is **yes**.
- **virtuals-depend-on-server-state**
  Specifies whether the system marks a virtual server down when the server on which the virtual server is configured can no longer be reached via iQuery. The default value is **yes**.

See Also

edit, *load-balancing*, *metrics*, *metrics-exclusions*, *list*, *modify*, *show*, *tmsh*

load-balancing

Configures the load balancing settings for the Global Traffic Manager™.

Syntax

Modify or display the **load-balancing** component within the **gtm global-settings** module using the syntax in the following sections.

Modify

```
modify load-balancing
    ignore-path-ttl [no | yes]
    respect-fallback-dependency [no | yes]
    topology-longest-match [no | yes]
    verify-vs-availability [no | yes]
edit load-balancing
    all-properties
    non-default-properties
```

Display

```
list
list load-balancing
show running-config load-balancing
show running-config load-balancing [option]
    all-properties
    non-default-properties
    one-line
```

Description

You can use the **load-balancing** component to modify or display the load balancing settings for the Global Traffic Manager.

Examples

modify load-balancing ignore-path-ttl yes

Specifies that dynamic load balancing methods can use path data, even after the time-to-live (TTL) for the path data expires.

list load-balancing all-properties

Displays all properties of the load balancing settings for the Global Traffic Manager.

Options

- **ignore-path-ttl**
  Specifies, when set to **yes**, that dynamic load balancing methods can use path data, even after the time-to-live (TTL) for the path data expires. The default value is **no**.
- **respect-fallback-dependency**
  Specifies, when set to **yes**, that the system accepts virtual server status when the load balancing mode changes to the mode specified by the **fallback-mode** option of the pool. The default value is **no**.
- **topology-longest-match**
  Specifies, when set to **yes**, that the system evaluates all topology records in the topology statement, and then selects the topology record that most specifically matches the IP address in an LDNS request (in other words, has the longest match). When this option is set to **no**, the system selects the first record in the topology statement that matches the request.
- **verify-vs-availability**
  Specifies, when set to **yes**, that the system checks the availability of virtual servers before sending a connection to those virtual servers. The default value is **no**.

See Also

edit, *general*, *metrics*, *metrics-exclusions*, *list*, *modify*, *show*, *tmsh*

metrics

Configures metrics for the Global Traffic Manager™.

Syntax

Modify or display the **metrics** component within the **gtm global-settings** module using the syntax in the following sections.

Modify

```
modify metrics
    default-probe-limit [integer]
    hops-ttl [integer]
    hops-packet-length [integer]
    hops-sample-count [integer]
    hops-timeout [integer]
    inactive-ldns-ttl [integer]
    ldns-update-interval [integer]
    inactive-paths-ttl [integer]
    max-synchronous-monitor-requests [integer]
    metrics-caching [integer]
    metrics-collection-protocols none
    metrics-collection-protocols
      [add | delete | replace-all-with] {
 [dns-dot | dns-rev | icmp | tcp | udp] ...
    }
    path-ttl [integer]
    paths-retry [integer]
edit metrics
   all-properties
   non-default-properties
   one-line
```

Display

```
list
list metrics
show running-config metrics
show running-config metrics [option]
    all-properties
    non-default-properties
```

Description

You can use the **metrics** component to modify or display the Global Traffic Manager metrics settings.

Examples

modify metrics default-probe-limit 10

Sets the default probe limit for the Global Traffic Manager to **10**.

list metrics all-properties

Displays all properties of the metrics settings for the Global Traffic Manager.

Options

- **default-probe-limit**
  Specifies the number of probe attempts that the system performs before removing the path from the metrics. The default value is **12**.
- **hops-ttl**
  Specifies the number of seconds that the system considers **traceroute** utility data to be valid for name resolution and load balancing. The default value is **604800**. Note that this option must be greater than the **hops-timeout** option.
- **hops-packet-length**
  Specifies the length of packets, in bytes, that the system sends to a local DNS server to determine the path information between the two systems. The default value is **64**.
- **hops-sample-count**
  Specifies the number of packets that the system sends to a local DNS server to determine the path information between those two systems. The default value is **3**.
- **hops-timeout**
  Specifies the number of seconds that the **big3d** daemon waits for a probe. The default value is **3**.
- **inactive-ldns-ttl**
  Specifies the number of seconds that an inactive LDNS remains in the cache. Each time an LDNS makes a request, the clock starts again. Valid values are **60** through **4294967295**. The default value is **2419200** (28 days).
- **ldns-update-interval**
  Specifies the number of seconds that a tmm will wait before sending an update for a LDNS which has been accessed. The default value is **20** seconds.
- **inactive-paths-ttl**
  Specifies the number of seconds that a path remains in the cache after its last access. Valid values are **60** through **4294967295**. The default value is **604800** (7 days).
- **max-synchronous-monitor-requests**
  Specifies how many monitors can attempt to verify the availability of a given resource at the same time. The default value is **20**.
- **metrics-caching**
  Specifies the interval (in seconds) at which the system dumps path and other metrics data. Valid values are **0** through **604800**. The default value is **3600**; **0** (zero) turns this feature off.

- **metrics-collection-protocols**
  Specifies the protocols that the system uses to collect metrics information relevant to LDNS servers.
- **path-ttl**
  Specifies the number of seconds that the system considers path data to be valid for name resolution and load balancing purposes. The default value is **2400**. Note that this option must be greater than the **paths-retry** option.
- **paths-retry**
  Specifies the interval (in seconds) at which the system retries the path data. The default value is **120**.

See Also

edit, *general*, *load-balancing*, *metrics-exclusions*, *list*, *modify*, *show*, *tmsh*

metrics-exclusions

Configures the IP addresses that you want to exclude from the Global Traffic Manager™ metrics.

Syntax

Modify or display the **metrics-exclusions** within the **gtm global-settings** module using the syntax in the following sections.

Modify

```
modify metrics-exclusions
    addresses [add | delete | none | replace-all-with] {
       [ip address]...
    }
edit metrics-exclusions
  all-properties
```

Display

```
list
list metrics-exclusions
show running-config metrics-exclusions
    addresses
    all-properties
    one-line
```

Description

You can use the **metrics-exclusions** component to exclude IP addresses from the Global Traffic Manager metrics.

Examples

modify metrics-exclusions addresses add {10.10.10.1}

Excludes the IP address **10.10.10.1** from inclusion in the Global Traffic Manager metrics.

list metrics-exclusions

Displays the IP addresses that are excluded from the Global Traffic Manager metrics.

Options

- **ip address**
  Specifies the IP addresses that you want to add to or delete from the exclusion list, or with which you want to replace all existing IP addresses that are currently on the exclusion list.

See Also

edit, *general*, *load-balancing*, *metrics*, *list*, *modify*, *show*, *tmsh*

48

gtm monitor

- Introducing the gtm monitor module
- Alphabetical list of components

Introducing the gtm monitor module

You can use the tmsh components that reside within the gtm monitor module to configure Global Traffic Manager™ monitors. For more information about the tmsh hierarchical structure, see Chapter 2, *Understanding and Using the Traffic Management Shell*.

For more information about configuring monitors, refer to the *Configuration Guide for BIG-IP® Global Traffic Manager™*.

Alphabetical list of components

The remainder of this chapter lists the tmsh components that are available in the gtm monitor module.

bigip

Configures a BIG-IP® monitor.

Syntax

Configure the **bigip** component within the **gtm monitor** module using the syntax in the following sections.

Create/Modify

```
create bigip [name]
modify bigip [name]
    aggregate-dynamic-ratios [average-members | average-nodes | none |
                              sum-members | sum-nodes]
    app-service [[string] | none]
    defaults-from [name]
    description [string]
    destination [ip address][port]
    ignore-down-response [enabled | disabled]
    interval [integer]
    timeout [integer]
edit bigip [ [name] | [glob] | [regex] ] ... ]
    all-properties
    non-default properties
```

Display

```
list bigip
list bigip [ [name] | [glob] | [regex] ] ... ]
show running-config bigip
show running-config bigip [ [name] | [glob] | [regex] ] ... ]
    all-properties
    non-default-properties
    one-line
    partition
```

Delete

```
delete bigip [name]
```

◆ Note

You cannot delete default monitors.

Description

You can use the **bigip** component in the **gtm monitor** module to configure a custom monitor, or you can use the default BIG-IP® monitor that the Global Traffic Manager™ provides. The BIG-IP monitor is both a health and performance monitor. This type of monitor acquires data captured through monitors managed by a BIG-IP Local Traffic Manager™.

You can monitor only the following components with a BIG-IP monitor:

- Global Traffic Manager server
- Global Traffic Manager virtual server
- Local Traffic Manager server
- Local Traffic Manager virtual server

Examples

create bigip my_bigip defaults-from bigip

Creates a monitor named **my_bigip** that inherits properties from the default BIG-IP monitor.

list bigip

Displays the properties of all of the BIG-IP monitors.

Options

- **aggregate-dynamic-ratios**
  Specifies the monitor's response to a query. By default, the BIG-IP monitor uses the gtm_score value as the vs_score for a Local Traffic Manager virtual server.
  You can use this option to override the default behavior using the following values:
  - **average-members**
    Specifies that the monitor uses the average of the dynamic ratio values of the pool members associated with the pools that are associated with the virtual server as a response to a query.
  - **average-nodes**
    Specifies that the monitor uses the average value of all of the nodes associated with the pool members that are associated with the pools that are associated with the virtual server as a response to a query.
  - **none**
    This is the default value.
  - **sum-members**
    Specifies that the monitor uses the sum of the pool members as a response to a query.
  - **sum-nodes**
    Specifies that the monitor uses the sum of the dynamic ratios of all of the nodes as a response to a query.
- **app-service**
  Specifies the name of the application service to which the monitor belongs. The default value is **none**. **Note:** If the **strict-updates** option is

enabled on the application service that owns the object, you cannot modify or delete the monitor. Only the application service can modify or delete the monitor.

- **defaults-from**
  Specifies the name of the monitor from which you want your custom monitor to inherit settings. The default value is **bigip**.
- **description**
  User defined description.
- **destination**
  Specifies the IP address and service port of the resource that is the destination of this monitor. The default value is *:*.
  Possible values are:
  - ***:***
    Specifies to perform a health check on the address and port supplied by a virtual server.
  - ***:port**
    Specifies to perform a health check on the virtual server with the IP address supplied by the virtual server and the port you specify.
  - **IP address:port**
    Specifies to mark a pool member **up** or **down** based on the response of the virtual server at the IP address and port you specify.
- **glob**
  Displays the items that match the **glob** expression. See **help glob** for a description of **glob** expression syntax.
- **ignore-down-response**
  Specifies whether the monitor ignores a down response from the system it is monitoring. The default value is **disabled**.
- **interval**
  Specifies the frequency at which the system issues the monitor check. The default value is **30** seconds.
- **name**
  Specifies a unique name for the component. This option is required for the commands **create**, **delete**, and **modify**.
- **partition**
  Displays the administrative partition within which the component resides.
- **regex**
  Displays the items that match the regular expression. The regular expression must be preceded by an at sign (@[regular expression]) to indicate that the identifier is a regular expression. See **help regex** for a description of regular expression syntax.
- **timeout**
  Specifies the number of seconds the target has in which to respond to the monitor request. The default value is **90** seconds.
  If the target responds within the set time period, it is considered **up**. If the target does not respond within the set time period, it is considered **down**.

Also, if the target responds with a RESET packet, the system immediately flags the target as **down** without waiting for the timeout interval to expire.

See Also

create, *delete*, *edit*, glob, *pool*, *server*, *list*, *modify*, regex, *show*, *tmsh*

bigip-link

Configures a BIG-IP® Link monitor.

Syntax

Configure the **bigip-link** component within the **gtm monitor** module using the syntax in the following sections.

Create/Modify

```
create bigip-link [name]
modify bigip-link [name]
    app-service [[string] | none]
    defaults-from [name]
    description [string]
    destination [ip address]
    ignore-down-response [enabled | disabled]
    interval [integer]
    timeout [integer]
edit bigip-link [ [ [name] | [glob] | [regex] ] ... ]
    all-properties
    non-default-properties
```

Display

```
list bigip-link
list bigip-link [ [ [name] | [glob] | [regex] ] ... ]
show running-config bigip-link
show running-config bigip-link [ [ [name] | [glob] | [regex] ] ... ]
    all-properties
    non-default-properties
    one-line
    partition
```

Delete

```
delete bigip-link [name]
```

◆ Note

You cannot delete default monitors.

Description

You can use the **bigip-link** component to configure a custom monitor, or you can use the default BIG-IP Link monitor that the Global Traffic Manager provides. This type of monitor acquires data captured through monitors managed by a BIG-IP Link Controller.

Examples

create bigip-link my_bigip-link defaults-from bigip_link

Creates a monitor named **my_bigip-link** that inherits properties from the default BIG-IP Link monitor.

list bigip-link

Displays the properties of all of the BIG-IP Link monitors.

Options

- **app-service**
  Specifies the name of the application service to which the monitor belongs. The default value is **none**. **Note:** If the **strict-updates** option is **enabled** on the application service that owns the object, you cannot modify or delete the monitor. Only the application service can modify or delete the monitor.
- **defaults-from**
  Specifies the name of the monitor from which you want your custom monitor to inherit settings. The default value is **bigip_link**.
- **description**
  User defined description.
- **destination**
  Specifies the IP address of the resource that is the destination of this monitor. The default value is *****.
  Possible values are:
  - *****
    Specifies to perform a health check on the IP address of the node.
  - **IP address**
    Specifies to perform a health check on the IP address that you specify, route the check through the IP address of the associated node, and mark the IP address of the associated node **up** or **down** accordingly.
- **glob**
  Displays the items that match the **glob** expression. See **help glob** for a description of **glob** expression syntax.
- **ignore-down-response**
  Specifies whether the monitor ignores a down response from the system it is monitoring. The default value is **disabled**.
- **interval**
  Specifies the frequency at which the system issues the monitor check. The default value is **10** seconds.
- **name**
  Specifies a unique name for the component. This option is required for the commands **create**, **delete**, and **modify**.
- **partition**
  Displays the administrative partition within which the component resides.

- **regex**
  Displays the items that match the regular expression. The regular expression must be preceded by an at sign (@[regular expression]) to indicate that the identifier is a regular expression. See **help regex** for a description of regular expression syntax.
- **timeout**
  Specifies the number of seconds the target has in which to respond to the monitor request. The default value is **30** seconds.
  If the target responds within the set time period, it is considered **up**. If the target does not respond within the set time period, it is considered **down**. Also, if the target responds with a RESET packet, the system immediately flags the target as **down** without waiting for the timeout interval to expire.

See Also

create, *delete*, *edit*, glob, *link*, *list*, *node*, *modify*, regex, *show*, *tmsh*,

external

Configures an external monitor.

Syntax

Configure the **external** component within the **gtm monitor** module using the syntax in the following sections.

Create/Modify

```
create external [name]
modify external [name]
    args [ [arguments] | none]
    defaults-from [name]
    description [string]
    destination [ip address][port]
    ignore-down-response [enabled | disabled]
    interval [integer]
    probe-timeout [integer]
    run [none | [path] ]
    timeout [integer]
    user-defined [ [name] [value] | [name] none ]
edit external [ [ [name] | [glob] | [regex] ] ... ]
    all-properties
    non-default-properties
```

Display

```
list external
list external [ [ [name] | [glob] | [regex] ] ... ]
show running-config external
show running-config external [ [ [name] | [glob] | [regex] ] ... ]
    all-properties
    non-default-properties
    one-line
    partition
```

Delete

```
delete external [name]
```

◆ Note

You cannot delete default monitors.

Description

You can use the **external** component to configure a custom monitor, or you can use the default external monitor that the Global Traffic Manager provides. You can use this type of monitor to monitor services using your own programs.

Examples

create external my_external defaults-from external

Creates a monitor named **my_external** that inherits properties from the default external monitor.

list external

Displays the properties of all of the external monitors.

Options

- **args**
  Specifies any command-line arguments that the external program requires. The default value is **none**.
- **defaults-from**
  Specifies the name of the monitor from which you want your custom monitor to inherit settings. The default value is **external**.
- **description**
  User defined description.
- **destination**
  Specifies the IP address and service port of the resource that is the destination of this monitor. The default value is ***:***.
  Possible values are:
  - ***:***
    Specifies to perform a health check on the IP address and port supplied by a pool member.
  - ***:port**
    Specifies to perform a health check on the server with the IP address supplied by the pool member and the port you specify.
  - **IP address:port**
    Specifies to mark a pool member **up** or **down** based on the response of the server at the IP address and port you specify.
- **glob**
  Displays the items that match the **glob** expression. See **help glob** for a description of **glob** expression syntax.
- **ignore-down-response**
  Specifies whether the monitor ignores a down response from the system it is monitoring. The default value is **disabled**.
- **interval**
  Specifies the frequency at which the system issues the monitor check. The default value is **30** seconds.
- **name**
  Specifies a unique name for the component. This option is required for the commands **create**, **delete**, and **modify**.
- **partition**
  Displays the administrative partition within which the component resides.

- **probe-timeout**
  Specifies the number of seconds after which the BIG-IP® system times out the probe request to the BIG-IP system. The default value is **5** seconds.
- **regex**
  Displays the items that match the regular expression. The regular expression must be preceded by an at sign (@[regular expression]) to indicate that the identifier is a regular expression. See **help regex** for a description of regular expression syntax.
- **run**
  Specifies the path and file name of a program to run as the external monitor, for example **/config/monitors/myMonitor**. The default value is **none**.
- **timeout**
  Specifies the number of seconds the target has in which to respond to the monitor request. The default value is **120** seconds.
  If the target responds within the set time period, it is considered **up**. If the target does not respond within the set time period, it is considered **down**. Also, if the target responds with a RESET packet, the system immediately flags the target as **down** without waiting for the timeout interval to expire.
- **user-defined**
  Specifies any user-defined command-line arguments and variables that the external program requires. Use the following syntax to specify a user defined parameter.

modify external my_external user-defined my_param_name my_param_value

Use the following syntax to remove a user defined parameter.

modify external my_external user-defined my_param_name none

See Also

create, *delete*, *edit*, glob, *pool*, *list*, *modify*, regex, *show*, *tmsh*,

firepass

Configures a FirePass® monitor.

Syntax

Configure the **firepass** component within the **gtm monitor** module using the syntax in the following sections.

Create/Modify

```
create firepass [name]
modify firepass [name]
    app-service [[string] | none]
    cipherlist [list]
    concurrency-limit [integer]
    defaults-from [name]
    description [string]
    destination [ip address][port]
    ignore-down-response [enabled | disabled]
    interval [integer]
    max-load-average [floating point value]
    password [none | [password] ]
    probe-timeout [integer]
    timeout [integer]
    username [name]
edit firepass [ [ [name] | [glob] | [regex] ] ... ]
    all-properties
    non-default-properties
```

Display

```
list firepass
list firepass [ [ [name] | [glob] | [regex] ] ... ]
show running-config firepass
show running-config firepass [ [ [name] | [glob] | [regex] ] ... ]
    all-properties
    non-default-properties
    one-line
    partition
```

Delete

```
delete firepass [name]
```

◆ Note

You cannot delete default monitors.

Description

You can use the **firepass** component to configure a custom monitor, or you can use the default FirePass monitor that the BIG-IP® Global Traffic Manager™ provides. The FirePass monitor is both a health and performance monitor.

For more information about configuring monitors, refer to the Configuration Guide for BIG-IP® Global Traffic Management.

Examples

create firepass my_firepass defaults-from firepass_gtm

Creates a monitor named **my_firepass** that inherits properties from the default FirePass monitor.

list firepass

Displays the properties of all of the FirePass monitors.

Options

- **app-service**
  Specifies the name of the application service to which the monitor belongs. The default value is **none**. **Note:** If the **strict-updates** option is **enabled** on the application service that owns the object, you cannot modify or delete the monitor. Only the application service can modify or delete the monitor.
- **cipherlist**
  Specifies the list of ciphers for this monitor. The default value is **HIGH:!ADH**.
- **concurrency-limit**
  Specifies the maximum percentage of licensed connections currently in use under which the monitor marks the FirePass system **up**. The default value is **95**.
  For example, a value of 95 percent means that the monitor marks the FirePass system **up** until 95 percent of licensed connections are in use. When the number of in-use licensed connections exceeds 95 percent, the monitor marks the FirePass system **down**.
- **defaults-from**
  Specifies the name of the monitor from which you want your custom monitor to inherit settings. The default value is **firepass_gtm**.
- **description**
  User defined description.
- **destination**
  Specifies the IP address and service port of the resource that is the destination of this monitor. The default value is ***:***.
  Possible values are:

- ***:***
  Specifies to perform a health check on the address and port supplied by a pool member.
- ***:port**
  Specifies to perform a health check on the server with the IP address supplied by the pool member and the port you specify.
- **IP address:port**
  Specifies to mark a pool member up or down based on the response of the server at the address you supply.

◆ **glob**
Displays the items that match the **glob** expression. See **help glob** for a description of **glob** expression syntax.

◆ **ignore-down-response**
Specifies whether the monitor ignores a down response from the system it is monitoring. The default value is **disabled**.

◆ **interval**
Specifies the frequency at which the system issues the monitor check. The default value is **30** seconds.

◆ **max-load-average**
Specifies the number that the monitor uses to mark the FirePass system up or down. The system compares value of this option against a one-minute average of the FirePass system load. When the FirePass system-load average falls within the specified value, the monitor marks the FirePass system **up**. When the average exceeds the setting, the monitor marks the system **down**.
The default value is **12.0**.

◆ **name**
Specifies a unique name for the component. This option is required for the commands **create**, **delete**, and **modify**.

◆ **partition**
Displays the administrative partition within which the component resides.

◆ **password**
Specifies the password, if the monitored target requires authentication. The default value is **none**.

◆ **probe-timeout**
Specifies the number of seconds after which the BIG-IP system times out the probe request to the BIG-IP system. The default value is **5** seconds.

◆ **regex**
Displays the items that match the regular expression. The regular expression must be preceded by an at sign (@[regular expression]) to indicate that the identifier is a regular expression. See **help regex** for a description of regular expression syntax.

◆ **timeout**
Specifies the number of seconds the target has in which to respond to the monitor request. The default value is **90** seconds.
If the target responds within the set time period, it is considered **up**. If the

target does not respond within the set time period, it is considered **down**. Also, if the target responds with a RESET packet, the system immediately flags the target as **down** without waiting for the timeout interval to expire.

- **username**
  Specifies the username, if the monitored target requires authentication. The default value is **gtmuser**.

See Also

create, *delete*, *edit*, glob, *pool*, *list*, *modify*, regex, *show*, *tmsh*

ftp

Configures a File Transfer Protocol (FTP) monitor.

Syntax

Configure the **ftp** component within the **gtm monitor** module using the syntax in the following sections.

Create/Modify

```
create ftp [name]
modify ftp [name]
    debug [no | yes]
    defaults-from [name]
    description [string]
    destination [ip address][port]
    filename [ [filename] | none]
    ignore-down-response [enabled | disabled]
    interval [integer]
    mode [passive | port]
    password [none | [password] ]
    probe-timeout [integer]
    timeout [integer]
    username [name]
edit ftp [ [ [name] | [glob] | [regex] ] ... ]
    all-properties
    non-default-properties
```

Display

```
list ftp
list ftp [ [ [name] | [glob] | [regex] ] ... ]
show running-config ftp
show running-config ftp [ [ [name] | [glob] | [regex] ] ... ]
    all-properties
    non-default-properties
    one-line
    partition
```

Delete

```
delete ftp [name]
```

◆ Note

You cannot delete default monitors.

Description

You can use the **ftp** component to configure a custom monitor, or you can use the default FTP monitor that the Global Traffic Manager provides. This type of monitor verifies the FTP service by attempting to download a specific file to the **/var/tmp** directory on the system. Once downloaded successfully, the file is not saved.

Examples

create ftp my_ftp defaults-from ftp

Creates a monitor named **my_ftp** that inherits properties from the default FTP monitor.

list ftp

Displays the properties of all of the FTP monitors.

Options

- **debug**
  Specifies whether the monitor sends error messages and additional information to a log file created and labeled specifically for this monitor. You can use the log information to help diagnose and troubleshoot unsuccessful health checks.
  The default value is **no**. The options are:
  - **no**
    Specifies that the system does not redirect error messages and additional information related to this monitor.
  - **yes**
    Specifies that the system redirects error messages and additional information to the /var/log/monitors/<monitor_name>-<node_name>-<port>.log file.
- **defaults-from**
  Specifies the name of the monitor from which you want your custom monitor to inherit settings. The default value is **ftp**.
- **description**
  User defined description.
- **destination**
  Specifies the IP address and service port of the resource that is the destination of this monitor. The default value is ***:***.
  Possible values are:
  - ***:***
    Specifies to perform a health check on the address and port supplied by a pool member.
  - ***:port**
    Specifies to perform a health check on the server with the IP address supplied by the pool member and the port you specify.

  - **IP address:port**
    Specifies to mark a pool member **up** or **down** based on the response of the server at the IP address and port you specify.

- **filename**
  Specifies the full path and file name of the file that the system attempts to download. The health check is successful if the system can download the file. The default value is **none**.
- **glob**
  Displays the items that match the **glob** expression. See **help glob** for a description of **glob** expression syntax.
- **ignore-down-response**
  Specifies whether the monitor ignores a down response from the system it is monitoring. The default value is **disabled**.
- **interval**
  Specifies the frequency at which the system issues the monitor check. The default value is **10** seconds.
- **mode**
  Specifies the data transfer process (DTP) mode. The default value is **passive**. The options are:
  - **passive**
    Specifies that the monitor sends a data transfer request to the FTP server. When the FTP server receives the request, the FTP server then starts and establishes the data connection.
  - **port**
    Specifies that the monitor starts and establishes the data connection with the FTP server.
- **name**
  Specifies a unique name for the component. This option is required for the commands **create**, **delete**, and **modify**.
- **password**
  Specifies the password, if the monitored target requires authentication. The default value is **none**.
- **partition**
  Displays the administrative partition within which the component resides.
- **probe-timeout**
  Specifies the number of seconds after which the BIG-IP® system times out the probe request to the BIG-IP system. The default value is **5** seconds.
- **regex**
  Displays the items that match the regular expression. The regular expression must be preceded by an at sign (@[regular expression]) to indicate that the identifier is a regular expression. See **help regex** for a description of regular expression syntax.
- **timeout**
  Specifies the number of seconds the target has in which to respond to the monitor request. The default value is **31** seconds.

If the target responds within the set time period, it is considered **up**. If the target does not respond within the set time period, it is considered **down**. Also, if the target responds with a RESET packet, the system immediately flags the target as **down** without waiting for the timeout interval to expire.

- **username**
  Specifies the username, if the monitored target requires authentication. The default value is **none**.

See Also

create, *delete*, *edit*, glob, *pool*, *list*, *modify*, regex, *show*, *tmsh*

gateway-icmp

Configures a Gateway Internet Control Message Protocol (ICMP) monitor.

Syntax

Configure the **gateway-icmp** component within the **gtm monitor** module using the syntax in the following sections.

Create/Modify

```
create gateway-icmp [name]
modify gateway-icmp [name]
    defaults-from [name]
    description [string]
    destination [ip address][port]
    ignore-down-response [enabled | disabled]
    interval [integer]
    probe-attempts [integer]
    probe-interval [integer]
    probe-timeout [integer]
    timeout [integer]
    transparent [enabled | disabled]
edit gateway-icmp [ [ [name] | [glob] | [regex] ] ... ]
    all-properties
    non-default-properties
```

Display

```
list gateway-icmp
list gateway-icmp [ [ [name] | [glob] | [regex] ] ... ]
show running-config gateway-icmp
show running-config gateway-icmp [ [ [name] | [glob] | [regex] ] ... ]
    all-properties
    non-default-properties
    one-line
    partition
```

Delete

```
delete gateway-icmp [name]
```

◆ Note

You cannot delete default monitors.

Description

You can use the **gateway-icmp** component to configure a custom monitor, or you can use the default Gateway ICMP monitor that the Global Traffic Manager provides. You can use a Gateway ICMP type of monitor for a

virtual server, a server (that is, all of the virtuals on a specified server), a pool member, a pool (that is, all of the pool members of a specified pool), or a link.

Examples

create gateway-icmp my_imcp defaults-from gateway_icmp

Creates a monitor named **my_icmp** that inherits properties from the default Gateway ICMP monitor.

list gateway-icmp

Displays the properties of all of the Gateway ICMP monitors.

Options

- **defaults-from**
  Specifies the name of the monitor from which you want your custom monitor to inherit settings. The default value is **gateway_icmp**.
- **description**
  User defined description.
- **destination**
  Specifies the IP address and service port of the resource that is the destination of this monitor. The default value is ***:***.
  Possible values are:
  - ***:***
    Specifies to perform a health check on the IP address and port supplied by a pool member.
  - ***:port**
    Specifies to perform a health check on the server with the IP address supplied by the pool member and the port you specify.
  - **IP address:port**
    Specifies to mark a pool member **up** or **down** based on the response of the server at the IP address and port you specify.
  - **IP address:port** (with the **transparent** option **enabled**)
    Specifies to perform a health check on the server at the IP address and port specified in the monitor, routing the check through the IP address and port supplied by the pool member. The pool member (the gateway) is marked **up** or **down** accordingly.
- **glob**
  Displays the items that match the **glob** expression. See **help glob** for a description of **glob** expression syntax.
- **ignore-down-response**
  Specifies whether the monitor ignores a down response from the system it is monitoring. The default value is **disabled**.

- **interval**
  Specifies the frequency at which the system issues the monitor check. The default value is **30** seconds.
- **name**
  Specifies a unique name for the component. This option is required for the commands **create**, **delete**, and **modify**.
- **partition**
  Displays the administrative partition within which the component resides.
- **probe-attempts**
  Specifies the number of times the BIG-IP® system attempts to probe the host server, after which the BIG-IP system considers the host server down or unavailable. The default value is **3** attempts.
- **probe-interval**
  Specifies the frequency at which the BIG-IP system probes the host server. The default value is **1** second.
- **probe-timeout**
  Specifies the number of seconds after which the BIG-IP system times out the probe request to the BIG-IP system. The default value is **5** seconds.
- **regex**
  Displays the items that match the regular expression. The regular expression must be preceded by an at sign (@[regular expression]) to indicate that the identifier is a regular expression. See **help regex** for a description of regular expression syntax.
- **timeout**
  Specifies the number of seconds the target has in which to respond to the monitor request. The default value is **120** seconds.
  If the target responds within the set time period, it is considered **up**. If the target does not respond within the set time period, it is considered **down**. Also, if the target responds with a RESET packet, the system immediately flags the target as **down** without waiting for the timeout interval to expire.
- **transparent**
  Specifies whether the monitor operates in transparent mode. Monitors in transparent mode can monitor pool members through firewalls. The default value is **disabled**.

See Also

create, *delete*, *edit*, glob, *link*, *pool*, *server*, *list*, *modify*, regex, *show*, *tmsh*

gtp

Configures a GPRS Tunneling Protocol (GTP) monitor. This monitor operates over UDP.

Syntax

Configure the **gtp** component within the **gtm monitor** module using the syntax in the following sections.

Create/Modify

```
create gtp [name]
modify gtp [name]
    defaults-from [name]
    description [string]
    destination [ip address][port]
    ignore-down-response [enabled | disabled]
    interval [integer]
    probe-attempts [integer]
    probe-interval [integer]
    probe-timeout [integer]
    protocol-version [integer]
    timeout [integer]
edit gtp [ [ [name] | [glob] | [regex] ] ... ]
    all-properties
    non-default-properties
```

Display

```
list gtp
list gtp [ [ [name] | [glob] | [regex] ] ... ]
show running-config gtp
show running-config gtp [ [ [name] | [glob] | [regex] ] ... ]
    all-properties
    non-default-properties
    one-line
    partition
```

Delete

```
delete gtp [name]
```

◆ Note

You cannot delete default monitors.

Description

You can use the **gtp** component to configure a custom monitor, or you can use the default GTP monitor that the Global Traffic Manager provides. This type of monitor verifies the GPRS tunneling service by attempting to send

GTP Echo Requests to a pool, pool member, or virtual server, and verifying the receipt of a well-formed Echo Response packet. This monitor supports GTP version 1 and version 2 over UDP.

For more information about configuring monitors, refer to the Configuration Guide for BIG-IP® Global Traffic Management.

Examples

create gtp my_gtp defaults-from gtp

Creates a monitor named **my_gtp** that inherits properties from the default GTP monitor.

list gtp

Displays the properties of all of the GTP monitors.

Options

- **defaults-from**
  Specifies the name of the monitor from which you want your custom monitor to inherit settings. The default value is **gtp**.
- **description**
  User defined description.
- **destination**
  Specifies the IP address and service port of the resource that is the destination of this monitor. Possible values are:
  - ***:***
    Specifies to perform a health check on the IP address and port supplied by a pool member.
  - ***:port**
    Specifies to perform a health check on the server with the IP address supplied by the pool member and the port you specify.
  - **IP address:port**
    Specifies to mark a pool member **up** or **down** based on the response of the server at the IP address and port you specify.
- **glob**
  Displays the items that match the **glob** expression. See **help glob** for a description of **glob** expression syntax.
- **ignore-down-response**
  Specifies whether the monitor ignores a down response from the system it is monitoring. The default value is **disabled**.
- **interval**
  Specifies the frequency at which the system issues the monitor check. The default value is **30** seconds.
- **name**
  Specifies a unique name for the component. This option is required for the commands **create**, **delete**, and **modify**.

- **partition**
  Displays the administrative partition within which the component resides.
- **probe-attempts**
  Specifies the number of times the BIG-IP system attempts to probe the host server, after which the BIG-IP system considers the host server down or unavailable. The default value is **3**.
- **probe-interval**
  Specifies the frequency at which the BIG-IP system probes the host server. The default value is **1**.
- **probe-timeout**
  Specifies the number of seconds after which the BIG-IP system times out the probe request to the BIG-IP system. The default value is **5** seconds.
- **protocol-version**
  Specifies the GTP protocol version used to perform the exchange. GTP version 1 and GTP version 2 are supported. The default is version 1.
- **regex**
  Displays the items that match the regular expression. The regular expression must be preceded by an at sign (@[regular expression]) to indicate that the identifier is a regular expression. See **help regex** for a description of regular expression syntax.
- **timeout**
  Specifies the number of seconds the target has in which to respond to the monitor request. The default value is **120** seconds. If the target responds within the set time period, it is considered up. If the target does not respond within the set time period, it is considered down. Also, if the target responds with a non-conforming Echo Reply, the system immediately flags the target as down without waiting for the timeout interval to expire.

See Also

create, *delete*, *edit*, glob, *pool*, *server*, *list*, *modify*, regex, *show*, *tmsh*

http

Configures a Hypertext Transfer Protocol (HTTP) monitor.

Syntax

Configure the **http** component within the **gtm monitor** module using the syntax in the following sections.

Create/Modify

```
create http [name]
modify http [name]
    defaults-from [name]
    description [string]
    destination [ip address][port]
    ignore-down-response [enabled | disabled]
    interval [integer]
    password [none | [password] ]
    probe-timeout [integer]
    recv [none | [string] ]
    reverse [enabled | disabled]
    send [none | [string] ]
    timeout [integer]
    transparent [enabled | disabled]
    username [ [name] | none]
edit http [ [ [name] | [glob] | [regex] ] ... ]
    all-properties
    non-default-properties
```

Display

```
list http
list http [ [ [name] | [glob] | [regex] ] ... ]
show running-config http
show running-config http [ [ [name] | [glob] | [regex] ] ... ]
    all-properties
    non-default-properties
    one-line
    partition
```

Delete

```
delete http [name]
```

◆ Note

You cannot delete default monitors.

Description

You can use the **http** component to configure a custom monitor, or you can use the default HTTP monitor that the Global Traffic Manager provides. This type of monitor verifies the HTTP service by attempting to receive specific content from a Web page.

Examples

create http my_http defaults-from http

Creates a monitor named **my_http** that inherits properties from the default HTTP monitor.

list http

Displays the properties of all of the HTTP monitors.

Options

- **defaults-from**
  Specifies the name of the monitor from which you want your custom monitor to inherit settings. The default value is **http**.
- **description**
  User defined description.
- **destination**
  Specifies the IP address and service port of the resource that is the destination of this monitor. The default value is ***:***.
  Possible values are:
  - ***:***
    Specifies to perform a health check on the IP address and port supplied by a pool member.
  - ***:port**
    Specifies to perform a health check on the server with the IP address supplied by the pool member and the port you specify.
  - **IP address:port**
    Specifies to mark a pool member **up** or **down** based on the response of the server at the IP address and port you specify.
  - **IP address:port** (with the **transparent** option **enabled**)
    Specifies to perform a health check on the server at the IP address and port specified in the monitor, routing the check through the IP address and port supplied by the pool member. The pool member (the gateway) is marked **up** or **down** accordingly.
- **glob**
  Displays the items that match the **glob** expression. See **help glob** for a description of **glob** expression syntax.

- **ignore-down-response**
  Specifies whether the monitor ignores a down response from the system it is monitoring. The default value is **disabled**.
- **interval**
  Specifies the frequency at which the system issues the monitor check. The default value is **30** seconds.
- **name**
  Specifies a unique name for the component. This option is required for the commands **create**, **delete**, and **modify**.
- **partition**
  Displays the administrative partition within which the component resides.
- **password**
  Specifies the password if the monitored target requires authentication. The default value is **none**.
- **probe-timeout**
  Specifies the number of seconds after which the BIG-IP® system times out the probe request to the BIG-IP system. The default value is **5** seconds.
- **recv**
  Specifies the text string that the monitor looks for in the returned resource. The default value is **none**.
  The most common receive expressions contain a text string that is included in an HTML file on your site. The text string can be regular text, HTML tags, or image names, and the associated operation is not case-sensitive. If you do not specify a value for both the **send** and **recv** options, the monitor performs a simple service check and connect only.
- **regex**
  Displays the items that match the regular expression. The regular expression must be preceded by an at sign (@[regular expression]) to indicate that the identifier is a regular expression. See **help regex** for a description of regular expression syntax.
- **reverse**
  Specifies whether the monitor operates in reverse mode. When the monitor is in reverse mode, a successful check marks the monitored object **down** instead of **up**. You can use the this mode only if you configure both the **send** and **recv** options.
  The default value is **disabled**, which specifies that the monitor does not operate in reverse mode. The **enabled** value specifies that the monitor operates in reverse mode.
- **send**
  Specifies the text string that the monitor sends to the target object.
  The default setting is **GET /**, which retrieves a default HTML file for a web site. To retrieve a specific page from a web site, specify a fully-qualified path name, for example, **GET /www/company/index.html**.
  Since the string may have special characters, the system may require that the string be enclosed with single quotation marks.

If this value is null, then a valid connection suffices to determine that the service is **up**. In this case, the system does not need the **recv** option and ignores the option even if not null.

- **timeout**
  Specifies the number of seconds the target has in which to respond to the monitor request. The default value is **120** seconds.
  If the target responds within the set time period, it is considered **up**. If the target does not respond within the set time period, it is considered **down**. Also, if the target responds with a RESET packet, the system immediately flags the target as **down** without waiting for the timeout interval to expire.
- **transparent**
  Specifies whether the monitor operates in transparent mode. Monitors in transparent mode can monitor pool members through firewalls. The default value is **disabled**.
- **username**
  Specifies the username, if the monitored target requires authentication. The default value is **none**.

See Also

create, *delete*, *pool*, *server*, *list*, *modify*, *show*, *tmsh*

https

Configures a Hypertext Transfer Protocol over Secure Socket Layer (HTTPS) monitor.

Syntax

Configure the **https** component within the **gtm monitor** module using the syntax in the following sections.

Create/Modify

```
create https [name]
modify https [name]
    cert [ [cert list] | none]
    cipherlist [string]
    compatibility [enabled | disabled]
    defaults-from [name]
    description [string]
    destination [ip address][port]
    ignore-down-response [enabled | disabled]
    interval [integer]
    key [ [key] | none]
    password [none | [password] ]
    probe-timeout [integer]
    recv [none | [string] ]
    reverse [enabled | disabled]
    send [none | [string] ]
    timeout [integer]
    transparent [enabled | disabled]
    username [ [name] | none]
edit https [ [ [name] | [glob] | [regex] ] ... ]
    all-properties
    non-default-properties
```

Display

```
list https
list https [ [ [name] | [glob] | [regex] ] ... ]
show running-config https
show running-config https [ [ [name] | [glob] | [regex] ] ... ]
    all-properties
    non-default-properties
    one-line
    partition
```

Delete

```
delete https [name]
```

◆ Note

You cannot delete default monitors.

Description

You can use the **http** component to configure a custom monitor, or you can use the default HTTPS monitor that the Global Traffic Manager provides. This type of monitor verifies the HTTPS service by attempting to receive specific content from a Web page protected by Secure Socket Layer (SSL) security.

Examples

create https my_https defaults-from https

Creates a monitor named **my_https** that inherits properties from the default HTTPS monitor.

list https

Displays the properties of all of the HTTPS monitors.

Options

- **cert**
  Specifies a fully-qualified path for a client certificate that the monitor sends to the target SSL server. The default value is **none**.
- **cipherlist**
  Specifies the list of ciphers for this monitor. The default list **DEFAULT:+SHA:+3DES:+kEDH** is located in the file **base_monitors.conf**.
- **compatibility**
  Specifies, when enabled, that the SSL options setting (in OpenSSL) is set to ALL. The default value is **enabled**.
- **defaults-from**
  Specifies the name of the monitor from which you want your custom monitor to inherit settings. The default value is **https**.
- **description**
  User defined description.
- **destination**
  Specifies the IP address and service port of the resource that is the destination of this monitor. The default value is ***:***.
  Possible values are:
  - ***:***
    Specifies to perform a health check on the IP address and port supplied by a pool member.
  - ***:port**
    Specifies to perform a health check on the server with the IP address supplied by the pool member and the port you specify.

- **IP address:port**
  Specifies to mark a pool member **up** or **down** based on the response of the server at the IP address and port you specify.
- **IP address:port** (with the **transparent** option **enabled**)
  Specifies to perform a health check on the server at the IP address and port specified in the monitor, routing the check through the IP address and port supplied by the pool member. The pool member (the gateway) is marked **up** or **down** accordingly.

◆ **glob**
Displays the items that match the **glob** expression. See **help glob** for a description of **glob** expression syntax.

◆ **ignore-down-response**
Specifies whether the monitor ignores a down response from the system it is monitoring. The default value is **disabled**.

◆ **interval**
Specifies the frequency at which the system issues the monitor check. The default value is **30** seconds.

◆ **key**
Specifies the RSA private key if the monitored target requires authentication. The key must be surrounded by quotation marks, for example, **key "client.key"**. Note that if you specify a key, you must also specify a value for the **cert** option. The default value is **none**.

◆ **name**
Specifies a unique name for the component. This option is required for the commands **create**, **delete**, and **modify**.

◆ **partition**
Displays the administrative partition within which the component resides.

◆ **password**
Specifies the password if the monitored target requires authentication. The default value is **none**.

◆ **probe-timeout**
Specifies the number of seconds after which the BIG-IP system times out the probe request to the BIG-IP system. The default value is **5** seconds.

◆ **recv**
Specifies the text string that the monitor looks for in the returned resource. The default value is **none**.
The most common receive expressions contain a text string that is included in an HTML file on your site. The text string can be regular text, HTML tags, or image names, and the associated operation is not case-sensitive. If you do not specify a value for both the **send** and **recv** options, the monitor performs a simple service check and connect only.

◆ **regex**
Displays the items that match the regular expression. The regular expression must be preceded by an at sign (@[regular expression]) to indicate that the identifier is a regular expression. See **help regex** for a description of regular expression syntax.

- **reverse**
  Specifies whether the monitor operates in reverse mode. When the monitor is in reverse mode, a successful check marks the monitored object **down** instead of **up**. You can use the this mode only if you configure both the **send** and **recv** options.
  The default value is **disabled**, which specifies that the monitor does not operate in reverse mode. The **enabled** value specifies that the monitor operates in reverse mode.
- **send**
  Specifies the text string that the monitor sends to the target object. The default value is **GET /**, which retrieves a default HTML file for a web site.
  To retrieve a specific page from a web site, specify a fully-qualified path name, for example, **GET /www/company/index.html**. Since the string may have special characters, the system may require that the string be enclosed with single quotation marks.
  If this value is null, then a valid connection suffices to determine that the service is **up**. In this case, the system does not need the **recv** option and ignores the option even if not null.
- **timeout**
  Specifies the number of seconds the target has in which to respond to the monitor request. The default value is **120** seconds.
  If the target responds within the set time period, it is considered **up**. If the target does not respond within the set time period, it is considered **down**. Also, if the target responds with a RESET packet, the system immediately flags the target as **down** without waiting for the timeout interval to expire.
- **transparent**
  Specifies whether the monitor operates in transparent mode. Monitors in transparent mode can monitor pool members through firewalls. The default value is **disabled**.
- **username**
  Specifies the username, if the monitored target requires authentication. The default value is **none**.

See Also

create, *delete*, *edit*, glob, *pool*, *list*, *modify*, regex, *show*, *tmsh*

imap

Configures an Internet Message Access Protocol (IMAP) monitor.

Syntax

Configure the **imap** component within the **gtm monitor** module using the syntax in the following sections.

Create/Modify

```
create imap [name]
modify imap [name]
    debug [no | yes]
    defaults-from [name]
    description [string]
    destination [ip address][port]
    folder [ [name] | none]
    ignore-down-response [enabled | disabled]
    interval [integer]
    password [none | [password] ]
    probe-timeout [integer]
    timeout [integer]
    transparent [enabled | disabled]
    username [ [name] | none]
edit imap [ [ [name] | [glob] | [regex] ] ... ]
    all-properties
    non-default-properties
```

Display

```
list imap
list imap [ [ [name] | [glob] | [regex] ] ... ]
show running-config imap
show running-config imap [ [ [name] | [glob] | [regex] ] ... ]
    all-properties
    non-default-properties
    one-line
    partition
```

Delete

```
delete imap [name]
```

◆ Note

You cannot delete default monitors.

Description

You can use the **imap** component to configure a custom monitor, or you can use the default IMAP monitor that the Global Traffic Manager provides. This type of monitor verifies IMAP by attempting to open a specified mail folder on a server. This monitor is similar to the POP3 monitor.

Examples

create imap my_imap defaults-from imap

Creates a monitor named **my_imap** that inherits properties from the default IMAP monitor.

list imap

Displays the properties of all of the IMAP monitors.

Options

- **debug**
  Specifies whether the monitor sends error messages and additional information to a log file created and labeled specifically for this monitor. You can use the log information to help diagnose and troubleshoot unsuccessful health checks.
  The default value is **no**. The options are:
  - **no**
    Specifies that the system does not redirect error messages and additional information related to this monitor.
  - **yes**
    Specifies that the system redirects error messages and additional information to the /var/log/monitors/<monitor_name>-<node_name>-<port>.log file.
- **defaults-from**
  Specifies the name of the monitor from which you want your custom monitor to inherit settings. The default value is **imap**.
- **description**
  User defined description.
- **destination**
  Specifies the IP address and service port of the resource that is the destination of this monitor. The default value is ***:***.
  Possible values are:
  - ***:***
    Specifies to perform a health check on the IP address and port supplied by a pool member.
  - ***:port**
    Specifies to perform a health check on the server with the IP address supplied by the pool member and the port you specify.

- **IP address:port**
  Specifies to mark a pool member **up** or **down** based on the response of the server at the IP address and port you specify.

- **glob**
  Displays the items that match the **glob** expression. See **help glob** for a description of **glob** expression syntax.
- **folder**
  Specifies the name of the folder on the IMAP server that the monitor tries to open. The default value is **INBOX**.
- **ignore-down-response**
  Specifies whether the monitor ignores a down response from the system it is monitoring. The default value is **disabled**.
- **interval**
  Specifies the frequency at which the system issues the monitor check. The default value is **10** seconds.
- **name**
  Specifies a unique name for the component. This option is required for the commands **create**, **delete**, and **modify**.
- **partition**
  Displays the administrative partition within which the component resides.
- **password**
  Specifies the password if the monitored target requires authentication. The default value is **none**.
- **probe-timeout**
  Specifies the number of seconds after which the BIG-IP® system times out the probe request to the BIG-IP system. The default value is **5** seconds.
- **regex**
  Displays the items that match the regular expression. The regular expression must be preceded by an at sign (@[regular expression]) to indicate that the identifier is a regular expression. See **help regex** for a description of regular expression syntax.
- **timeout**
  Specifies the number of seconds the target has in which to respond to the monitor request. The default value is **31** seconds.
  If the target responds within the set time period, it is considered **up**. If the target does not respond within the set time period, it is considered **down**. Also, if the target responds with a RESET packet, the system immediately flags the target as **down** without waiting for the timeout interval to expire.
- **transparent**
  Specifies whether the monitor operates in transparent mode. Monitors in transparent mode can monitor pool members through firewalls. The default value is **disabled**.

- **username**
  Specifies the username, if the monitored target requires authentication. The default value is **none**.

See Also

create, *delete*, *edit*, glob, *pool*, *list*, *modify*, regex, *show*, *tmsh*

ldap

Configures a Lightweight Directory Access Protocol (LDAP) monitor.

Syntax

Configure the **ldap** component within the **gtm monitor** module using the syntax in the following sections.

Create/Modify

```
create ldap [name]
modify ldap [name]
    base [none | [string] ]
    chase-referrals [ no | yes ]
    debug [no | yes]
    defaults-from [name]
    description [string]
    destination [ip address][port]
    filter [ [LDAP key] | none]
    ignore-down-response [enabled | disabled]
    interval [integer]
    mandatory-attributes [no | yes]
    password [none | [password] ]
    probe-timeout [integer]
    security [none | ssl | tls]
    timeout [integer]
    username [ [name] | none]
edit ldap [ [ [name] | [glob] | [regex] ] ... ]
    all-properties
    non-default-properties
```

Display

```
list ldap
list ldap [ [ [name] | [glob] | [regex] ] ... ]
show running-config ldap
show running-config ldap [ [ [name] | [glob] | [regex] ] ... ]
    all-properties
    non-default-properties
    one-line
    partition
```

Delete

```
delete ldap [name]
```

◆ Note

You cannot delete default monitors.

Description

You can use the **ldap** component to configure a custom monitor, or you can use the default LDAP monitor that the Global Traffic Manager provides. This type of monitor verifies the LDAP service by attempting to authenticate the specified user.

Examples

create ldap my_ldap defaults-from ldap

Creates a monitor named **my_ldap** that inherits properties from the default LDAP monitor.

list ldap

Displays the properties of all of the LDAP monitors.

Options

- **base**
  Specifies the location in the LDAP tree from which the monitor starts the health check. A sample value is **dc=bigip-test,dc=net**. The default value is **none**.
- **chase-referrals**
  Specifies whether the monitor upon receipt of an LDAP referral entry chases that referral. The default value is **yes**.
  The options are:
  - **no**
    Specifies that the system will treat a referral entry as a normal entry and refrain from querying the remote LDAP server(s) pointed to by the referral entry.
  - **yes**
    Specifies that the system upon receiving any referral entry from the monitored LDAP server query, the system will then query the corresponding LDAP server(s) pointed to by the LDAP query. If the query for the referral is unsuccessful the system will mark the monitored LDAP server down.
- **debug**
  Specifies whether the monitor sends error messages and additional information to a log file created and labeled specifically for this monitor. You can use the log information to help diagnose and troubleshoot unsuccessful health checks.
  The default value is **no**. The options are:
  - **no**
    Specifies that the system does not redirect error messages and additional information related to this monitor.

- **yes**
  Specifies that the system redirects error messages and additional information to the /var/log/monitors/<monitor_name>-<node_name>-<port>.log file.

◆ **defaults-from**
Specifies the name of the monitor from which you want your custom monitor to inherit settings. The default value is **ldap**.

◆ **description**
User defined description.

◆ **destination**
Specifies the IP address and service port of the resource that is the destination of this monitor. The default value is ***:***.
Possible values are:

- ***:***
  Specifies to perform a health check on the address and port supplied by a pool member.
- ***:port**
  Specifies to perform a health check on the server with the IP address supplied by the pool member and the port you specify.
- **IP address:port**
  Specifies to mark a pool member **up** or **down** based on the response of the server at the IP address and port you specify.

◆ **filter**
Specifies an LDAP key for which the monitor searches. A sample value is **objectclass=***. The default value is **none**.

◆ **glob**
Displays the items that match the **glob** expression. See **help glob** for a description of **glob** expression syntax

◆ **ignore-down-response**
Specifies whether the monitor ignores a down response from the system it is monitoring. The default value is **disabled**.

◆ **interval**
Specifies the frequency at which the system issues the monitor check. The default value is **10** seconds.

◆ **mandatory-attributes**
Specifies whether the target must include attributes in its response to be considered **up**. The default value is **no**. The options are:

- **no**
  Specifies that the system performs only a one-level search (based on the value of the **filter** option), and does not require that the target returns any attributes.
- **yes**
  Specifies that the system performs a sub-tree search, and if the target returns no attributes, the target is considered down.

◆ **name**
Specifies a unique name for the component. This option is required for the commands **create**, **delete**, and **modify**.

- **partition**
  Displays the administrative partition within which the component resides.
- **password**
  Specifies the password if the monitored target requires authentication. The default value is **none**.
- **probe-timeout**
  Specifies the number of seconds after which the BIG-IP® system times out the probe request to the BIG-IP system. The default value is **5** seconds.
- **regex**
  Displays the items that match the regular expression. The regular expression must be preceded by an at sign (@[regular expression]) to indicate that the identifier is a regular expression. See **help regex** for a description of regular expression syntax.
- **security**
  Specifies the secure communications protocol that the monitor uses to communicate with the target. The default value is **none**.
  The options are:
  - **none**
    Specifies that the system does not use a security protocol for communications with the target.
  - **ssl**
    Specifies that the system uses the SSL protocol for communications with the target.
  - **tls**
    Specifies that the system uses the TLS protocol for communications with the target.
- **timeout**
  Specifies the number of seconds the target has in which to respond to the monitor request. The default value is **31** seconds.
  If the target responds within the set time period, it is considered **up**. If the target does not respond within the set time period, it is considered **down**. Also, if the target responds with a RESET packet, the system immediately flags the target as **down** without waiting for the timeout interval to expire.
- **username**
  Specifies the username, if the monitored target requires authentication. The default value is **none**.

See Also

create, *delete*, *edit*, glob, *pool*, *list*, *modify*, regex, *show*, *tmsh*

mssql

Configures a Microsoft® Windows® Structured Query Language (MSSQL) monitor.

Syntax

Configure the **mssql** component within the **gtm monitor** module using the syntax in the following sections.

Create/Modify

```
create mssql [name]
modify mssql [name]
    count [0 | 1]
    database [ [name] | none]
    debug [no | yes]
    defaults-from [name]
    description [string]
    destination [ip address][port]
    ignore-down-response [enabled | disabled]
    interval [integer]
    password [none | [password] ]
    probe-timeout [integer]
    recv [none | [string] ]
    recv-column [none | [string] ]
    recv-row [none | [string] ]
    send [none | [string] ]
    timeout [integer]
    username [ [name] | none]
edit mssql [ [ [name] | [glob] | [regex] ] ... ]
    all-properties
    non-default-properties
```

Display

```
list mssql
list mssql [ [ [name] | [glob] | [regex] ] ... ]
show running-config mssql
show running-config mssql [ [ [name] | [glob] | [regex] ] ... ]
    all-properties
    non-default-properties
    one-line
    partition
```

Delete

```
delete mssql [name]
```

◆ Note

You cannot delete default monitors.

Description

You can use the **mssql** component to configure a custom monitor, or you can use the default MSSQL monitor that the Global Traffic Manager provides. This type of monitor verifies Microsoft Windows SQL-based services.

Examples

create mssql my_mssql defaults-from mssql

Creates a monitor named **my_mssql** that inherits properties from the default MSSQL monitor.

list mssql

Displays the properties of all of the MSSQL monitors.

Options

- **count**
  Specifies the number of instances for which the system keeps a connection open. By default, when you assign instances of this monitor to a resource, the system keeps the connection to the database open. With this option you can assign multiple instances to the database while reducing the overhead that multiple open connections can cause.
  A value of **0** (zero), the default, keeps the connection open for all instances. A value of **1** opens a new connection for each instance. Any other positive value keeps the connection open for that many instances; for example, a value of **5** keeps the connection open for five instances of this monitor.
- **database**
  Specifies the name of the database with which the monitor attempts to communicate. The default value is **none**.
- **debug**
  Specifies whether the monitor sends error messages and additional information to a log file created and labeled specifically for this monitor. You can use the log information to help diagnose and troubleshoot unsuccessful health checks. The default value is **no**.
  The options are:
  - **no**
    Specifies that the system does not redirect error messages and additional information related to this monitor.
  - **yes**
    Specifies that the system redirects error messages and additional information to the /var/log/monitors/<monitor_name>-<node_name>-<port>.log file.

- **defaults-from**
  Specifies the name of the monitor from which you want your custom monitor to inherit settings. The default value is **mssql**.
- **description**
  User defined description.
- **destination**
  Specifies the IP address and service port of the resource that is the destination of this monitor. The default value is ***:***.
  Possible values are:
  - ***:***
    Specifies to perform a health check on the IP address and port supplied by a pool member.
  - ***:port**
    Specifies to perform a health check on the server with the IP address supplied by the pool member and the port you specify.
  - **IP address:port**
    Specifies to mark a pool member **up** or **down** based on the response of the server at the IP address and port you specify.
- **glob**
  Displays the items that match the **glob** expression. See **help glob** for a description of **glob** expression syntax.
- **ignore-down-response**
  Specifies whether the monitor ignores a down response from the system it is monitoring. The default value is **disabled**.
- **interval**
  Specifies the frequency at which the system issues the monitor check. The default value is **30** seconds.
- **name**
  Specifies a unique name for the component. This option is required for the commands **create**, **delete**, and **modify**.
- **partition**
  Displays the administrative partition within which the component resides.
- **password**
  Specifies the password if the monitored target requires authentication. The default value is **none**.
- **probe-timeout**
  Specifies the number of seconds after which the BIG-IP® system times out the probe request to the BIG-IP system. The default value is **5** seconds.
- **recv**
  Specifies the text string that the monitor looks for in the returned resource. The default value is **none**.
  The most common receive expressions contain a text string that is included in a field in your database. If you do not specify a value for both the **send** and **recv** options, the monitor performs a simple service check and connect only.

- **recv-column**
  Specifies the column in the database where the system expects the specified Receive String to be located. Specify this option only if you configure the **send** and **recv** options. The default value is **none**.
- **recv-row**
  Specifies the row in the database where the system expects the specified Receive String to be located. Specify this option only if you configure the **send** and **recv** options. The default value is **none**.
- **regex**
  Displays the items that match the regular expression. The regular expression must be preceded by an at sign (@[regular expression]) to indicate that the identifier is a regular expression. See **help regex** for a description of regular expression syntax.
- **send**
  Specifies the SQL query that the monitor sends to the target database, for example, **SELECT count(*) FROM mytable**.
  If this value is null, then a valid connection suffices to determine that the service is **up**. In this case, the system does not need the **recv** option and ignores the option even if not null.
- **timeout**
  Specifies the number of seconds the target has in which to respond to the monitor request. The default value is **91** seconds.
  If the target responds within the set time period, it is considered **up**. If the target does not respond within the set time period, it is considered **down**. Also, if the target responds with a RESET packet, the system immediately flags the target as **down** without waiting for the timeout interval to expire.
- **username**
  Specifies the username, if the monitored target requires authentication. The default value is **none**.

See Also

create, *delete*, *edit*, glob, *pool*, *list*, *modify*, regex, *show*, *tmsh*

mysql

Configures a MySQL® monitor.

Syntax

Configure the **mysql** component within the **gtm monitor** module using the syntax in the following sections.

Create/Modify

```
create mysql [name]
modify mysql [name]
    count [0 | 1]
    database [ [name] | none]
    debug [no | yes]
    defaults-from [name]
    description [string]
    destination [ip address][port]
    ignore-down-response [enabled | disabled]
    interval [integer]
    password [none | [password] ]
    probe-timeout [integer]
    recv [none | [string] ]
    recv-column [none | [string] ]
    recv-row [none | [string] ]
    send [none | [string] ]
    timeout [integer]
    username [ [name] | none]
edit mysql [ [ [name] | [glob] | [regex] ] ... ]
    all-properties
    non-default-properties
```

Display

```
list mysql
list mysql [ [ [name] | [glob] | [regex] ] ... ]
show running-config mysql
show running-config mysql [ [ [name] | [glob] | [regex] ] ... ]
    all-properties
    non-default-properties
    one-line
    partition
```

Delete

```
delete mysql [name]
```

◆ Note

You cannot delete default monitors.

Description

You can use the **mysql** component to configure a custom monitor, or you can use the default MySQL monitor that the Global Traffic Manager provides. This type of monitor verifies Microsoft® Windows® SQL-based services.

Examples

create mysql my_mysql defaults-from mysql

Creates a monitor named **my_mysql** that inherits properties from the default MySQL monitor.

list mysql

Displays the properties of all of the MySQL monitors.

Options

- **count**
  Specifies the number of instances for which the system keeps a connection open. By default, when you assign instances of this monitor to a resource, the system keeps the connection to the database open. With this option you can assign multiple instances to the database while reducing the overhead that multiple open connections can cause.
  A value of **0** (zero), the default, keeps the connection open for all instances. A value of **1** opens a new connection for each instance. Any other positive value keeps the connection open for that many instances; for example, a value of **5** keeps the connection open for five instances of this monitor.
- **database**
  Specifies the name of the database with which the monitor attempts to communicate. The default value is **none**.
- **debug**
  Specifies whether the monitor sends error messages and additional information to a log file created and labeled specifically for this monitor. You can use the log information to help diagnose and troubleshoot unsuccessful health checks. The default value is **no**.
  The options are:
  - **no**
    Specifies that the system does not redirect error messages and additional information related to this monitor.
  - **yes**
    Specifies that the system redirects error messages and additional information to the /var/log/monitors/<monitor_name>-<node_name>-<port>.log file.

- **defaults-from**
  Specifies the name of the monitor from which you want your custom monitor to inherit settings. The default value is **mysql**.
- **description**
  User defined description.
- **destination**
  Specifies the IP address and service port of the resource that is the destination of this monitor. The default value is ***:***.
  Possible values are:
  - ***:***
    Specifies to perform a health check on the IP address and port supplied by a pool member.
  - ***:port**
    Specifies to perform a health check on the server with the IP address supplied by the pool member and the port you specify.
  - **IP address:port**
    Specifies to mark a pool member **up** or **down** based on the response of the server at the IP address and port you specify.
- **glob**
  Displays the items that match the **glob** expression. See **help glob** for a description of **glob** expression syntax.
- **ignore-down-response**
  Specifies whether the monitor ignores a down response from the system it is monitoring. The default value is **disabled**.
- **interval**
  Specifies the frequency at which the system issues the monitor check. The default value is **30** seconds.
- **name**
  Specifies a unique name for the component. This option is required for the commands **create**, **delete**, and **modify**.
- **partition**
  Displays the administrative partition within which the component resides.
- **password**
  Specifies the password if the monitored target requires authentication. The default value is **none**.
- **probe-timeout**
  Specifies the number of seconds after which the BIG-IP® system times out the probe request to the BIG-IP system. The default value is **5** seconds.
- **recv**
  Specifies the text string that the monitor looks for in the returned resource. The default value is **none**.
  The most common receive expressions contain a text string that is included in a field in your database. If you do not specify a value for both the **send** and **recv** options, the monitor performs a simple service check and connect only.

- **recv-column**
  Specifies the column in the database where the system expects the specified Receive String to be located. Specify this option only if you configure the **send** and **recv** options. The default value is **none**.
- **recv-row**
  Specifies the row in the database where the system expects the specified Receive String to be located. Specify this option only if you configure the **send** and **recv** options. The default value is **none**.
- **regex**
  Displays the items that match the regular expression. The regular expression must be preceded by an at sign (@[regular expression]) to indicate that the identifier is a regular expression. See **help regex** for a description of regular expression syntax.
- **send**
  Specifies the SQL query that the monitor sends to the target database, for example, **SELECT count(*) FROM mytable**.
  If this value is null, then a valid connection suffices to determine that the service is **up**. In this case, the system does not need the **recv** option and ignores the option even if not null.
- **timeout**
  Specifies the number of seconds the target has in which to respond to the monitor request. The default value is **91** seconds.
  If the target responds within the set time period, it is considered **up**. If the target does not respond within the set time period, it is considered **down**. Also, if the target responds with a RESET packet, the system immediately flags the target as **down** without waiting for the timeout interval to expire.
- **username**
  Specifies the username, if the monitored target requires authentication. The default value is **none**.

See Also

create, *delete*, *edit*, glob, *pool*, *list*, *modify*, regex, *show*, *tmsh*

nntp

Configures a Network News Transfer Protocol (NNTP) monitor.

Syntax

Configure the **nntp** component within the **gtm monitor** module using the syntax in the following sections.

Create/Modify

```
create nntp [name]
modify nntp [name]
    debug [no | yes]
    defaults-from [name]
    description [string]
    destination [ip address][port]
    ignore-down-response [enabled | disabled]
    interval [integer]
    newsgroup [ [name] | none]
    password [none | [password] ]
    probe-timeout [integer]
    timeout [integer]
    username [ [name] | none]
edit nntp [ [ [name] | [glob] | [regex] ] ... ]
    all-properties
    non-default-properties
```

Display

```
list nntp
list nntp [ [ [name] | [glob] | [regex] ] ... ]
show running-config nntp
show running-config nntp [ [ [name] | [glob] | [regex] ] ... ]
    all-properties
    non-default-properties
    one-line
    partition
```

Delete

```
delete nntp [name]
```

◆ Note

You cannot delete default monitors.

Description

You can use the **nntp** component to configure a custom monitor, or you can use the default NNTP monitor that the Global Traffic Manager provides. This type of monitor verifies the Usenet News protocol service by attempting to retrieve a newsgroup identification string from the server.

Examples

create nntp my_nntp defaults-from nntp

Creates a monitor named **my_nntp** that inherits properties from the default NNTP monitor.

list nntp

Displays the properties of all of the NNTP monitors.

Options

- **debug**
  Specifies whether the monitor sends error messages and additional information to a log file created and labeled specifically for this monitor. You can use the log information to help diagnose and troubleshoot unsuccessful health checks. The default value is **no**.
  The options are:
  - **no**
    Specifies that the system does not redirect error messages and additional information related to this monitor.
  - **yes**
    Specifies that the system redirects error messages and additional information to the /var/log/monitors/<monitor_name>-<node_name>-<port>.log file.
- **defaults-from**
  Specifies the name of the monitor from which you want your custom monitor to inherit settings. The default value is **nntp**.
- **description**
  User defined description.
- **destination**
  Specifies the IP address and service port of the resource that is the destination of this monitor. The default value is ***:***.
  Possible values are:
  - ***:***
    Specifies to perform a health check on the IP address and port supplied by a pool member.
  - ***:port**
    Specifies to perform a health check on the server with the IP address supplied by the pool member and the port you specify.

- **IP address:port**
  Specifies to mark a pool member **up** or **down** based on the response of the server at the IP address and port you specify.

- **glob**
  Displays the items that match the **glob** expression. See **help glob** for a description of **glob** expression syntax.
- **ignore-down-response**
  Specifies whether the monitor ignores a down response from the system it is monitoring. The default value is **disabled**.
- **interval**
  Specifies the frequency at which the system issues the monitor check. The default value is **30** seconds.
- **name**
  Specifies a unique name for the component. This option is required for the commands **create**, **delete**, and **modify**.
- **newsgroup**
  Specifies the name of the newsgroup that you are monitoring, for example **alt.car.mercedes**. The default value is **none**.
- **partition**
  Displays the administrative partition within which the component resides.
- **password**
  Specifies the password if the monitored target requires authentication. The default value is **none**.
- **probe-timeout**
  Specifies the number of seconds after which the BIG-IP® system times out the probe request to the BIG-IP system. The default value is **5** seconds.
- **regex**
  Displays the items that match the regular expression. The regular expression must be preceded by an at sign (@[regular expression]) to indicate that the identifier is a regular expression. See **help regex** for a description of regular expression syntax.
- **timeout**
  Specifies the number of seconds the target has in which to respond to the monitor request. The default value is **120** seconds.
  If the target responds within the set time period, it is considered **up**. If the target does not respond within the set time period, it is considered **down**. Also, if the target responds with a RESET packet, the system immediately flags the target as **down** without waiting for the timeout interval to expire.
- **username**
  Specifies the username, if the monitored target requires authentication. The default value is **none**.

See Also

create, *delete*, *edit*, glob, *pool*, *list*, *modify*, regex, *show*, *tmsh*

oracle

Configures an Oracle® monitor.

Syntax

Configure the **oracle** component within the **gtm monitor** module using the syntax in the following sections.

Create/Modify

```
create oracle [name]
modify oracle [name]
    count [0 | 1]
    database [ [name] | none]
    debug [no | yes]
    defaults-from [name]
    description [string]
    destination [ip address][port]
    ignore-down-response [enabled | disabled]
    interval [integer]
    password [none | [password] ]
    probe-timeout [integer]
    recv [none | [string] ]
    recv-column [none | [string] ]
    recv-row [none | [string] ]
    send [none | [string] ]
    timeout [integer]
    username [ [name] | none]
edit oracle [ [ [name] | [glob] | [regex] ] ... ]
    all-properties
    non-default-properties
```

Display

```
list oracle
list oracle [ [ [name] | [glob] | [regex] ] ... ]
show running-config oracle
show running-config oracle [ [ [name] | [glob] | [regex] ] ... ]
    all-properties
    non-default-properties
    one-line
    partition
```

Delete

```
delete oracle [name]
```

◆ Note

You cannot delete default monitors.

Description

You can use the **oracle** component to configure a custom monitor, or you can use the default Oracle monitor that the Global Traffic Manager provides. This type of monitor verifies services based on Oracle by attempting to perform an Oracle login to a service.

Examples

create oracle my_oracle defaults-from oracle

Creates a monitor named **my_oracle** that inherits properties from the default Oracle monitor.

list oracle

Displays the properties of all of the Oracle monitors.

Options

- **count**
  Specifies the number of instances for which the system keeps a connection open. By default, when you assign instances of this monitor to a resource, the system keeps the connection to the database open. With this option you can assign multiple instances to the database while reducing the overhead that multiple open connections can cause.
  A value of **0** (zero), the default, keeps the connection open for all instances. A value of **1** opens a new connection for each instance. Any other positive value keeps the connection open for that many instances; for example, a value of **5** keeps the connection open for five instances of this monitor.
- **database**
  Specifies the name of the database with which the monitor attempts to communicate. The default value is **none**.
- **debug**
  Specifies whether the monitor sends error messages and additional information to a log file created and labeled specifically for this monitor. You can use the log information to help diagnose and troubleshoot unsuccessful health checks. The default value is **no**.
  The options are:
  - **no**
    Specifies that the system does not redirect error messages and additional information related to this monitor.
  - **yes**
    Specifies that the system redirects error messages and additional information to the /var/log/monitors/<monitor_name>-<node_name>-<port>.log file.

- **defaults-from**
  Specifies the name of the monitor from which you want your custom monitor to inherit settings. The default value is **oracle**.
- **description**
  User defined description.
- **destination**
  Specifies the IP address and service port of the resource that is the destination of this monitor. The default value is ***:***.
  Possible values are:
  - ***:***
    Specifies to perform a health check on the IP address and port supplied by a pool member.
  - ***:port**
    Specifies to perform a health check on the server with the IP address supplied by the pool member and the port you specify.
  - **IP address:port**
    Specifies to mark a pool member **up** or **down** based on the response of the server at the IP address and port you specify.
- **glob**
  Displays the items that match the **glob** expression. See **help glob** for a description of **glob** expression syntax.
- **ignore-down-response**
  Specifies whether the monitor ignores a down response from the system it is monitoring. The default value is **disabled**.
- **interval**
  Specifies the frequency at which the system issues the monitor check. The default value is **30** seconds.
- **name**
  Specifies a unique name for the component. This option is required for the commands **create**, **delete**, and **modify**.
- **partition**
  Displays the administrative partition within which the component resides.
- **password**
  Specifies the password if the monitored target requires authentication. The default value is **none**.
- **probe-timeout**
  Specifies the number of seconds after which the BIG-IP® system times out the probe request to the BIG-IP system. The default value is **5** seconds.
- **recv**
  Specifies the text string that the monitor looks for in the returned resource. The default value is **none**.
  The most common receive expressions contain a text string that is included in a field in your database. If you do not specify a value for both the **send** and **recv** options, the monitor performs a simple service check and connect only.

- **recv-column**
  Specifies the column in the database where the system expects the specified Receive String to be located. Specify this option only if you configure the **send** and **recv** options. The default value is **none**.
- **recv-row**
  Specifies the row in the database where the system expects the specified Receive String to be located. Specify this option only if you configure the **send** and **recv** options. The default value is **none**.
- **regex**
  Displays the items that match the regular expression. The regular expression must be preceded by an at sign (@[regular expression]) to indicate that the identifier is a regular expression. See **help regex** for a description of regular expression syntax.
- **send**
  Specifies the SQL query that the monitor sends to the target database, for example, **SELECT count(*) FROM mytable**.
  If this value is null, then a valid connection suffices to determine that the service is **up**. In this case, the system does not need the recv option and ignores the option even if not null.
- **timeout**
  Specifies the number of seconds the target has in which to respond to the monitor request. The default value is **91** seconds.
  If the target responds within the set time period, it is considered **up**. If the target does not respond within the set time period, it is considered **down**. Also, if the target responds with a RESET packet, the system immediately flags the target as **down** without waiting for the timeout interval to expire.
- **username**
  Specifies the username, if the monitored target requires authentication. The default value is **none**.

See Also

create, *delete*, *edit*, glob, *pool*, *list*, *modify*, regex, *show*, *tmsh*

pop3

Configures a Post Office Protocol version 3 (POP3) monitor.

Syntax

Configure the **pop3** component within the **gtm monitor** module using the syntax in the following sections.

Create/Modify

```
create pop3 [name]
modify pop3 [name]
    debug [no | yes]
    defaults-from [name]
    description [string]
    destination [ip address][port]
    ignore-down-response [enabled | disabled]
    interval [integer]
    password [none | [password] ]
    probe-timeout [integer]
    timeout [integer]
    username [ [name] | none]
edit pop3 [ [ [name] | [glob] | [regex] ] ... ]
    all-properties
    non-default-properties
```

Display

```
list pop3
list pop3 [ [ [name] | [glob] | [regex] ] ... ]
show running-config pop3
show running-config pop3 [ [ [name] | [glob] | [regex] ] ... ]
    all-properties
    non-default-properties
    one-line
    partition
```

Delete

```
delete pop3 [name]
```

◆ Note

You cannot delete default monitors.

Description

You can use the **pop3** component to configure a custom monitor, or you can use the default POP3 monitor that the Global Traffic Manager provides. This type of monitor verifies the POP3 service by attempting to connect to a pool, pool member, or virtual server, log on as the specified user, and log off.

Examples

create pop3 my_pop3 defaults-from pop3

Creates a monitor named **my_pop3** that inherits properties from the default POP3 monitor.

list pop3

Displays the properties of all of the POP3 monitors.

Options

- **debug**
  Specifies whether the monitor sends error messages and additional information to a log file created and labeled specifically for this monitor. You can use the log information to help diagnose and troubleshoot unsuccessful health checks. The default value is **no**.
  The options are:
  - **no**
    Specifies that the system does not redirect error messages and additional information related to this monitor.
  - **yes**
    Specifies that the system redirects error messages and additional information to the /var/log/monitors/<monitor_name>-<node_name>-<port>.log file.
- **defaults-from**
  Specifies the name of the monitor from which you want your custom monitor to inherit settings. The default value is **pop3**.
- **description**
  User defined description.
- **destination**
  Specifies the IP address and service port of the resource that is the destination of this monitor. The default value is ***:***.
  Possible values are:
  - ***:***
    Specifies to perform a health check on the IP address and port supplied by a pool member.
  - ***:port**
    Specifies to perform a health check on the server with the IP address supplied by the pool member and the port you specify.

- **IP address:port**
  Specifies to mark a pool member **up** or **down** based on the response of the server at the IP address and port you specify.

- **glob**
  Displays the items that match the **glob** expression. See **help glob** for a description of **glob** expression syntax.
- **ignore-down-response**
  Specifies whether the monitor ignores a down response from the system it is monitoring. The default value is **disabled**.
- **interval**
  Specifies the frequency at which the system issues the monitor check. The default value is **30** seconds.
- **name**
  Specifies a unique name for the component. This option is required for the commands **create**, **delete**, and **modify**.
- **partition**
  Displays the administrative partition within which the component resides.
- **password**
  Specifies the password if the monitored target requires authentication. The default value is **none**.
- **probe-timeout**
  Specifies the number of seconds after which the BIG-IP® system times out the probe request to the BIG-IP system. The default value is **5** seconds.
- **regex**
  Displays the items that match the regular expression. The regular expression must be preceded by an at sign (@[regular expression]) to indicate that the identifier is a regular expression. See **help regex** for a description of regular expression syntax.
- **timeout**
  Specifies the number of seconds the target has in which to respond to the monitor request. The default value is **120** seconds.
  If the target responds within the set time period, it is considered **up**. If the target does not respond within the set time period, it is considered **down**. Also, if the target responds with a RESET packet, the system immediately flags the target as **down** without waiting for the timeout interval to expire.
- **username**
  Specifies the username, if the monitored target requires authentication. The default value is **none**.

See Also

create, *delete*, *edit*, glob, *pool*, *list*, *modify*, regex, *show*, *tmsh*

postgresql

Configures a PostgreSQL® monitor.

Syntax

Configure the **postgresql** component within the **gtm monitor** module using the syntax in the following sections.

Create/Modify

```
create postgresql [name]
modify postgresql [name]
    count [0 | 1]
    database [ [name] | none]
    debug [no | yes]
    defaults-from [name]
    description [string]
    destination [ip address][port]
    ignore-down-response [enabled | disabled]
    interval [integer]
    password [none | [password] ]
    probe-timeout [integer]
    recv [none | [string] ]
    recv-column [none | [string] ]
    recv-row [none | [string] ]
    send [none | [string] ]
    timeout [integer]
    username [ [name] | none]
edit postgresql [ [ [name] | [glob] | [regex] ] ... ]
    all-properties
    non-default-properties
```

Display

```
list postgresql
list postgresql [ [ [name] | [glob] | [regex] ] ... ]
show running-config postgresql
show running-config postgresql [ [ [name] | [glob] | [regex] ] ... ]
    all-properties
    non-default-properties
    one-line
    partition
```

Delete

```
delete postgresql [name]
```

◆ Note

You cannot delete default monitors.

Description

You can use the **postgresql** component to configure a custom monitor, or you can use the default PostgreSQL monitor that the Global Traffic Manager provides. This type of monitor verifies Microsoft® Windows® SQL-based services.

Examples

create postgresql my_postgresql defaults-from postgresql

Creates a monitor named **my_postgresql** that inherits properties from the default PostgreSQL monitor.

list postgresql

Displays the properties of all of the PostgreSQL monitors.

Options

- **count**
  Specifies the number of instances for which the system keeps a connection open. By default, when you assign instances of this monitor to a resource, the system keeps the connection to the database open. With this option you can assign multiple instances to the database while reducing the overhead that multiple open connections can cause.
  A value of **0** (zero), the default, keeps the connection open for all instances. A value of **1** opens a new connection for each instance. Any other positive value keeps the connection open for that many instances; for example, a value of **5** keeps the connection open for five instances of this monitor.
- **database**
  Specifies the name of the database with which the monitor attempts to communicate. The default value is **none**.
- **debug**
  Specifies whether the monitor sends error messages and additional information to a log file created and labeled specifically for this monitor. You can use the log information to help diagnose and troubleshoot unsuccessful health checks. The default value is **no**.
  The options are:
  - **no**
    Specifies that the system does not redirect error messages and additional information related to this monitor.
  - **yes**
    Specifies that the system redirects error messages and additional information to the /var/log/monitors/<monitor_name>-<node_name>-<port>.log file.

- **defaults-from**
  Specifies the name of the monitor from which you want your custom monitor to inherit settings. The default value is **postgresql**.
- **description**
  User defined description.
- **destination**
  Specifies the IP address and service port of the resource that is the destination of this monitor. The default value is ***:***.
  Possible values are:
  - ***:***
    Specifies to perform a health check on the IP address and port supplied by a pool member.
  - ***:port**
    Specifies to perform a health check on the server with the IP address supplied by the pool member and the port you specify.
  - **IP address:port**
    Specifies to mark a pool member **up** or **down** based on the response of the server at the IP address and port you specify.
- **glob**
  Displays the items that match the **glob** expression. See **help glob** for a description of **glob** expression syntax.
- **ignore-down-response**
  Specifies whether the monitor ignores a down response from the system it is monitoring. The default value is **disabled**.
- **interval**
  Specifies the frequency at which the system issues the monitor check. The default value is **30** seconds.
- **name**
  Specifies a unique name for the component. This option is required for the commands **create**, **delete**, and **modify**.
- **partition**
  Displays the administrative partition within which the component resides.
- **password**
  Specifies the password if the monitored target requires authentication. The default value is **none**.
- **probe-timeout**
  Specifies the number of seconds after which the BIG-IP® system times out the probe request to the BIG-IP system. The default value is **5** seconds.
- **recv**
  Specifies the text string that the monitor looks for in the returned resource. The default value is **none**.
  The most common receive expressions contain a text string that is included in a field in your database. If you do not specify a value for both the **send** and **recv** options, the monitor performs a simple service check and connect only.

- **recv-column**
  Specifies the column in the database where the system expects the specified Receive String to be located. Specify this option only if you configure the **send** and **recv** options. The default value is **none**.
- **recv-row**
  Specifies the row in the database where the system expects the specified Receive String to be located. Specify this option only if you configure the **send** and **recv** options. The default value is **none**.
- **regex**
  Displays the items that match the regular expression. The regular expression must be preceded by an at sign (@[regular expression]) to indicate that the identifier is a regular expression. See **help regex** for a description of regular expression syntax.
- **send**
  Specifies the SQL query that the monitor sends to the target database, for example, **SELECT count(*) FROM mytable**.
  If this value is null, then a valid connection suffices to determine that the service is **up**. In this case, the system does not need the **recv** option and ignores the option even if not null.
- **timeout**
  Specifies the number of seconds the target has in which to respond to the monitor request. The default value is **91** seconds.
  If the target responds within the set time period, it is considered **up**. If the target does not respond within the set time period, it is considered **down**. Also, if the target responds with a RESET packet, the system immediately flags the target as **down** without waiting for the timeout interval to expire.
- **username**
  Specifies the username, if the monitored target requires authentication. The default value is **none**.

See Also

create, *delete*, *edit*, glob, *pool*, *list*, *modify*, regex, *show*, *tmsh*

radius

Configures a Remote Access Dial-in User Service (RADIUS) monitor.

Syntax

Configure the **radius** component within the **gtm monitor** module using the syntax in the following sections.

Create/Modify

```
create radius [name]
modify radius [name]
    debug [no | yes]
    defaults-from [name]
    description [string]
    destination [ip address][port]
    ignore-down-response [enabled | disabled]
    interval [integer]
    nas-ip-address [ [ip address] | none]
    password [none | [password] ]
    probe-timeout [integer]
    secret [none | [secret] ]
    timeout [integer]
    username [ [name] | none]
edit radius [ [ [name] | [glob] | [regex] ] ... ]
    all-properties
    non-default-properties
```

Display

```
list radius
list radius [ [ [name] | [glob] | [regex] ] ... ]
show running-config radius
show running-config radius [ [ [name] | [glob] | [regex] ] ... ]
    all-properties
    non-default-properties
    one-line
    partition
```

Delete

```
delete radius [name]
```

◆ Note

You cannot delete default monitors.

Description

You can use the **radius** component to configure a custom monitor, or you can use the default RADIUS monitor that the Global Traffic Manager provides. This type of monitor verifies the RADIUS service by attempting to authenticate the specified user.

Examples

create radius my_radius defaults-from radius

Creates a monitor named **my_radius** that inherits properties from the default RADIUS monitor.

list radius

Displays the properties of all of the RADIUS monitors.

Options

- **debug**
  Specifies whether the monitor sends error messages and additional information to a log file created and labeled specifically for this monitor. You can use the log information to help diagnose and troubleshoot unsuccessful health checks. The default value is **no**.
  The options are:
  - **no**
    Specifies that the system does not redirect error messages and additional information related to this monitor.
  - **yes**
    Specifies that the system redirects error messages and additional information to the /var/log/monitors/<monitor_name>-<node_name>-<port>.log file.
- **defaults-from**
  Specifies the name of the monitor from which you want your custom monitor to inherit settings. The default value is **radius**.
- **description**
  User defined description.
- **destination**
  Specifies the IP address and service port of the resource that is the destination of this monitor. The default value is ***:***.
  Possible values are:
  - ***:***
    Specifies to perform a health check on the IP address and port supplied by a pool member.
  - ***:port**
    Specifies to perform a health check on the server with the IP address supplied by the pool member and the port you specify.

- **IP address:port**
  Specifies to mark a pool member **up** or **down** based on the response of the server at the IP address and port you specify.

- **glob**
  Displays the items that match the **glob** expression. See **help glob** for a description of **glob** expression syntax.
- **ignore-down-response**
  Specifies whether the monitor ignores a down response from the system it is monitoring. The default value is **disabled**.
- **interval**
  Specifies the frequency at which the system issues the monitor check. The default value is **30** seconds.
- **name**
  Specifies a unique name for the component. This option is required for the commands **create**, **delete**, and **modify**.
- **nas-ip-address**
  Specifies the network access server IP address that the system uses to identify itself to the RADIUS server. Using this option, multiple BIG-IP® systems can appear as a single network access device to the RADIUS server. The default value is **none**.
- **partition**
  Displays the administrative partition within which the component resides.
- **password**
  Specifies the password if the monitored target requires authentication. The default value is **none**.
- **probe-timeout**
  Specifies the number of seconds after which the BIG-IP system times out the probe request to the BIG-IP system. The default value is **5** seconds.
- **regex**
  Displays the items that match the regular expression. The regular expression must be preceded by an at sign (@[regular expression]) to indicate that the identifier is a regular expression. See **help regex** for a description of regular expression syntax.
- **secret**
  Specifies the secret the monitor needs to communicate with the resource. The default value is **none**.
- **timeout**
  Specifies the number of seconds the target has in which to respond to the monitor request. The default value is **31** seconds.
  If the target responds within the set time period, it is considered **up**. If the target does not respond within the set time period, it is considered **down**. Also, if the target responds with a RESET packet, the system immediately flags the target as **down** without waiting for the timeout interval to expire.

- **username**
  Specifies the username, if the monitored target requires authentication. The default value is **none**.

See Also

create, *delete*, *edit*, glob, *pool*, *list*, *modify*, regex, *show*, *tmsh*

radius-accounting

Configures a RADIUS accounting monitor for the BIG-IP® Global Traffic Manager.

Syntax

Configure the **radius-accounting** component within the **gtm monitor** module using the syntax shown in the following sections.

Create/Modify

```
create radius-accounting [name]
modify radius [name]
    check-until-up [disabled | enabled]
    debug [no | yes]
    defaults-from [ [name] | none]
    description [string]
    destination [ip address]
    interval [integer]
    manual-resume [disabled | enabled]
    nas-ip-address [ip address]
    secret [string]
    time-until-up [integer]
    timeout [integer]
    username [none | [string] ]
edit radius-accounting [ [ [name] | [glob] | [regex] ] ...]
     all-properties
     non-default-properties
```

Display

```
list radius-accounting
list radius-accounting [ [ [name] | [glob] | [regex] ] ...]
show running-config radius
show running-config radius [ [ [name] | [glob] | [regex] ] ...]
    all-properties
    non-default-properties
    one-line
    partition
```

Delete

```
delete radius-accounting [name]
```

◆ Note

You cannot delete default monitors.

Description

You can use the **radius-accounting** component to configure a custom monitor, or you can use the default RADIUS accounting monitor that the Global Traffic Manager provides. This type of monitor provides information about the usage of the RADIUS service for accounting purposes.

Examples

create radius-accounting my_radius_acct defaults-from radius_accounting

Creates a monitor named **my_radius_acct** that inherits properties from the default RADIUS accounting monitor.

list radius-accounting

Displays the properties of all of the RADIUS accounting monitors.

Options

- **check-until-up**
  When **enabled**, specifies that when an active and passive (inband) monitor are combined in an AND type of rule, the active monitor performs health checks only when the pool member is **down**, or until the pool member is marked as **up**. When the passive monitor marks the pool member **down**, the active monitor resumes health checks.
  The default value is **disabled**.
- **debug**
  Specifies whether the monitor sends error messages and additional information to a log file created and labeled specifically for this monitor. You can use the log information to help diagnose and troubleshoot unsuccessful health checks. The default value is **no**.
  The options are:
  - **no**
    Specifies that the system does not redirect error messages and additional information related to this monitor.
  - **yes**
    Specifies that the system redirects error messages and additional information to the /var/log/monitors/<monitor_name>-<node_name>-<port>.log file.
- **defaults-from**
  Specifies the name of the monitor from which you want your custom monitor to inherit settings. The default value is **radius**.
- **description**
  User defined description.

- **destination**
  Specifies the IP address and service port of the resource that is the destination of this monitor. The default value is ***:***.
  Possible values are:
  - ***:***
    Specifies to perform a health check on the IP address and port supplied by a pool member.
  - ***:port**
    Specifies to perform a health check on the server with the IP address supplied by the pool member and the port you specify.
  - **IP address:port**
    Specifies to mark a pool member **up** or **down** based on the response of the server at the IP address and port you specify.
- **glob**
  Displays the items that match the **glob** expression. See **help glob** for a description of **glob** expression syntax.
- **interval**
  Specifies the frequency at which the system issues the monitor check. The default value is **10** seconds.
- **manual-resume**
  Specifies whether the system automatically changes the status of a resource to **up** at the next successful monitor check. The default value of the **manual-resume** option is **disabled**.
  Note that if you set the **manual-resume** option to **enabled**, you must manually mark the resource as **up** before the system can use it for load balancing connections.
- **name**
  Specifies a unique name for the component. This option is required for the commands **create**, **delete**, and **modify**.
- **nas-ip-address**
  Specifies the network access server IP address that the system uses to identify itself to the RADIUS server. Using this option, multiple BIG-IP® systems can appear as a single network access device to the RADIUS server. The default value is **none**.
- **partition**
  Displays the administrative partition within which the component resides.
- **regex**
  Displays the items that match the regular expression. The regular expression must be preceded by an at sign (@[regular expression]) to indicate that the identifier is a regular expression. See **help regex** for a description of regular expression syntax.
- **secret**
  Specifies the secret the monitor needs to communicate with the resource. The default value is **none**.

- **time-until-up**
  Specifies the amount of time in seconds after the first successful response before a node is marked up. A value of **0** (zero) causes a node to be marked up immediately after a valid response is received from the node. The default value is **0** (zero).
- **timeout**
  Specifies the number of seconds the target has in which to respond to the monitor request. The default value is **31** seconds.
  If the target responds within the set time period, it is considered **up**. If the target does not respond within the set time period, it is considered **down**. Also, if the target responds with a RESET packet, the system immediately flags the target as **down** without waiting for the timeout interval to expire.
- **username**
  Specifies the username, if the monitored target requires authentication. The default value is **none**.

See Also

create, *delete*, *edit*, glob, *pool*, *list*, *modify*, regex, *show*, *tmsh*

real-server

Configures a RealServer® monitor.

Syntax

Configure the **real-server** component within the **gtm monitor** module using the syntax in the following sections.

Create/Modify

```
create real-server [name]
modify real-server [name]
    defaults-from [name]
    description [string]
    ignore-down-response [enabled | disabled]
    interval [integer]
    metrics [ [metrics] | none]
    probe-timeout [integer]
    timeout [integer]
edit real-server [ [ [name] | [glob] | [regex] ] ... ]
    all-properties
    non-default-properties
```

Display

```
list real-server
list real-server [ [ [name] | [glob] | [regex] ] ... ]
show running-config real-server
show running-config real-server [ [ [name] | [glob] | [regex] ] ... ]
    agent
    all-properties
    command
    method
    non-default-properties
    one-line
    partition
```

Delete

```
delete real-server [name]
```

◆ Note

You cannot delete default monitors.

Description

You can use the **real-server** component to configure a custom monitor, or you can use the default RealServer monitor that the Global Traffic Manager provides. This type of monitor checks the performance of a pool, pool member, or virtual server that is running the RealServer data collection agent, and then dynamically load balances traffic accordingly.

Examples

create real-server my_real-server defaults-from real_server

Creates a monitor named **my_real-server** that inherits properties from the default RealServer monitor.

list real-server

Displays the properties of all of the RealServer monitors.

Options

- **agent**
  Displays the agent for the monitor. The default agent is **Mozilla/4.0 (compatible: MSIE 5.0; Windows NT)**. You cannot modify the agent.
- **command**
  Displays the command that the system uses to obtain the metrics from the resource. See the documentation for this resource for information on available commands. You cannot modify the command.
- **defaults-from**
  Specifies the name of the monitor from which you want your custom monitor to inherit settings. The default value is **real_server**.
- **description**
  User defined description.
- **glob**
  Displays the items that match the **glob** expression. See **help glob** for a description of **glob** expression syntax.
- **ignore-down-response**
  Specifies whether the monitor ignores a down response from the system it is monitoring. The default value is **disabled**.
- **interval**
  Specifies the frequency at which the system issues the monitor check. The default value is **30** seconds.
- **name**
  Specifies a unique name for the component. This option is required for the commands **create**, **delete**, and **modify**.
- **method**
  Displays the GET method. You cannot modify the method.

- **metrics**
  Specifies the performance metrics that the commands collect from the target. The default value is **ServerBandwidth:1.5, CPUPercentUsage, MemoryUsage, TotalClientCount**.
- **partition**
  Displays the administrative partition within which the component resides.
- **probe-timeout**
  Specifies the number of seconds after which the BIG-IP® system times out the probe request to the BIG-IP system. The default value is **5** seconds.
- **regex**
  Displays the items that match the regular expression. The regular expression must be preceded by an at sign (@[regular expression]) to indicate that the identifier is a regular expression. See **help regex** for a description of regular expression syntax.
- **timeout**
  Specifies the number of seconds the target has in which to respond to the monitor request. The default value is **120** seconds.
  If the target responds within the set time period, it is considered **up**. If the target does not respond within the set time period, it is considered **down**. Also, if the target responds with a RESET packet, the system immediately flags the target as **down** without waiting for the timeout interval to expire.

See Also

create, *delete*, *edit*, glob, *pool*, *server*, *list*, *node*, *modify*, regex, *show*, *tmsh*

scripted

Configures a Scripted monitor.

Syntax

Configure the **scripted** component within the **gtm monitor** module using the syntax in the following sections.

Create/Modify

```
create scripted [name]
modify scripted [name]
    debug [no | yes]
    defaults-from [name]
    description [string]
    destination [ip address][port]
    filename [ [filename] | none]
    ignore-down-response [enabled | disabled]
    interval [integer]
    probe-timeout [integer]
    timeout [integer]
edit scripted [ [ [name] | [glob] | [regex] ] ... ]
    all-properties
    non-default-properties
```

Display

```
list scripted
list scripted [ [ [name] | [glob] | [regex] ] ... ]
show running-config scripted
show running-config scripted [ [ [name] | [glob] | [regex] ] ... ]
    all-properties
    non-default-properties
    one-line
    partition
```

Delete

```
delete scripted [name]
```

◆ Note

You cannot delete default monitors.

Description

You can use the **scripted** component to configure a custom monitor, or you can use the default scripted monitor that the Global Traffic Manager provides.

Examples

create scripted my_scripted defaults-from scripted

Creates a monitor named **my_scripted** that inherits properties from the default Scripted monitor.

list scripted

Displays the properties of all of the scripted monitors.

Options

- **debug**
  Specifies whether the monitor sends error messages and additional information to a log file created and labeled specifically for this monitor. You can use the log information to help diagnose and troubleshoot unsuccessful health checks. The default value is **no**.
  The options are:
  - **no**
    Specifies that the system does not redirect error messages and additional information related to this monitor.
  - **yes**
    Specifies that the system redirects error messages and additional information to the /var/log/monitors/<monitor_name>-<node_name>-<port>.log file.
- **defaults-from**
  Specifies the name of the monitor from which you want your custom monitor to inherit settings. The default value is **scripted**.
- **description**
  User defined description.
- **destination**
  Specifies the IP address and service port of the resource that is the destination of this monitor. The default value is ***:***.
  Possible values are:
  - ***:***
    Specifies to perform a health check on the IP address and port supplied by a pool member.
  - ***:port**
    Specifies to perform a health check on the server with the IP address supplied by the pool member and the port you specify.
  - **IP address:port**
    Specifies to mark a pool member **up** or **down** based on the response of the server at the IP address and port you specify.
- **filename**
  Specifies the name of a file in the **/config/eav/** directory on the system. The user-created file contains the send and expect data that the monitor uses for the monitor check. The default value is **none**.

- **glob**
  Displays the items that match the **glob** expression. See **help glob** for a description of **glob** expression syntax.
- **ignore-down-response**
  Specifies whether the monitor ignores a down response from the system it is monitoring. The default value is **disabled**.
- **interval**
  Specifies the frequency at which the system issues the monitor check. The default value is **10** seconds.
- **name**
  Specifies a unique name for the component. This option is required for the commands **create**, **delete**, and **modify**.
- **partition**
  Displays the administrative partition within which the component resides.
- **probe-timeout**
  Specifies the number of seconds after which the BIG-IP® system times out the probe request to the BIG-IP system. The default value is **5** seconds.
- **regex**
  Displays the items that match the regular expression. The regular expression must be preceded by an at sign (@[regular expression]) to indicate that the identifier is a regular expression. See **help regex** for a description of regular expression syntax.
- **timeout**
  Specifies the number of seconds the target has in which to respond to the monitor request. The default value is **31** seconds.
  If the target responds within the set time period, it is considered **up**. If the target does not respond within the set time period, it is considered **down**. Also, if the target responds with a RESET packet, the system immediately flags the target as **down** without waiting for the timeout interval to expire.

See Also

create, *delete*, *edit*, glob, *pool*, *list*, *modify*, regex, *show*, *tmsh*

sip

Configures a Session Initiation Protocol (SIP) monitor.

Syntax

Configure the **sip** component within the **gtm monitor** module using the syntax in the following sections.

Create/Modify

```
create sip [name]
modify sip [name]
    cert [ [cert list] | none]
    cipherlist [list]
    compatibility [enabled | disabled]
    debug [ no | yes]
    defaults-from [name]
    description [string]
    destination [ip address][port]
    filter [any | none | status]
    filter-neg [any | none | status]
    headers [ [new line separated headers] | none]
    ignore-down-response [enabled | disabled]
    interval [integer]
    key [ [key] | none]
    mode [sips | tcp | tls | udp]
    probe-timeout [integer]
    request [none | [string] ]
    username [ [name] | none]
edit sip [ [ [name] | [glob] | [regex] ] ... ]
    all-properties
    non-default-properties
```

Display

```
list sip
list sip [ [ [name] | [glob] | [regex] ] ... ]
show running-config sip
show running-config sip [ [ [name] | [glob] | [regex] ] ... ]
    all-properties
    non-default-properties
    one-line
    partition
```

Delete

```
delete sip [name]
```

◆ Note

You cannot delete default monitors.

Description

You can use the **sip** component to configure a custom monitor, or you can use the default SIP monitor that the Global Traffic Manager provides. This type of monitor checks the status of SIP Call-ID services on a device. The SIP protocol enables real-time messaging, voice, data, and video.

Examples

create sip my_sip defaults-from sip

Creates a monitor named **my_sip** that inherits properties from the default SIP monitor.

list sip

Displays the properties of all of the SIP monitors.

Options

- **cert**
  Specifies a fully-qualified path for a client certificate that the monitor sends to the target SSL server. The default value is **none**.
- **cipherlist**
  Specifies the list of ciphers for this monitor. The default value is **none**.
- **compatibility**
  Specifies, when enabled, that the SSL options setting (in OpenSSL) is set to ALL. The default value is **enabled**.
- **debug**
  Specifies whether the monitor sends error messages and additional information to a log file created and labeled specifically for this monitor. You can use the log information to help diagnose and troubleshoot unsuccessful health checks. The default value is **no**.
  The options are:
  - **no**
    Specifies that the system does not redirect error messages and additional information related to this monitor.
  - **yes**
    Specifies that the system redirects error messages and additional information to the /var/log/monitors/<monitor_name>-<node_name>-<port>.log file.
- **defaults-from**
  Specifies the name of the monitor from which you want your custom monitor to inherit settings. The default value is **sip**.
- **description**
  User defined description.

- **destination**
  Specifies the IP address and service port of the resource that is the destination of this monitor. The default value is ***:***.
  Possible values are:
  - ***:***
    Specifies to perform a health check on the IP address and port supplied by a pool member.
  - ***:port**
    Specifies to perform a health check on the server with the IP address supplied by the pool member and the port you specify.
  - **IP address:port**
    Specifies to mark a pool member **up** or **down** based on the response of the server at the IP address and port you specify.
- **filter**
  Specifies the SIP status codes that the target can return to be considered **up**. By default the system always accepts status codes whose value is in the 100s, 200s, or 300s.
  The options are:
  - **any**
    Specifies that the monitor accepts any SIP status codes.
  - **none**
    Specifies that the monitor does not accept any other SIP status codes. This is the default value.
  - **status**
    Specifies one or more status codes that you want to add to the monitor.
- **filter-neg**
  Specifies the SIP status codes that the target can return to be considered **down**. By default the system always accepts status codes according to **sip-monitor.filter**. After checking that, the status code is checked against this key. If a code is also in **sip-monitor.filter**, the node is marked **up**.
  The options are:
  - **any**
    Specifies that the monitor rejects all SIP status codes that are not in **sip-monitor.filter**.
  - **none**
    Specifies that the monitor does not specifically reject any other SIP status codes. This is the default value.
  - **status**
    Specifies one or more status codes that you want to add to the monitor.
- **glob**
  Displays the items that match the **glob** expression. See **help glob** for a description of **glob** expression syntax.

- **headers**
  Specifies the set of SIP headers in the SIP message that is sent to the target. Separate each header with a new line. The default value is **none**.
- **ignore-down-response**
  Specifies whether the monitor ignores a down response from the system it is monitoring. The default value is **disabled**.
- **interval**
  Specifies the frequency at which the system issues the monitor check. The default value is **30** seconds.
- **key**
  Specifies the key if the monitored target requires authentication. The default value is **none**.
- **mode**
  Specifies the protocol that the monitor uses to communicate with the target. The options are:
  - **sips**
    Specifies that the monitor uses SIPS to communicate with the target.
  - **tcp**
    Specifies that the monitor uses TCP to communicate with the target.
  - **tls**
    Specifies that the monitor uses TLS to communicate with the target, and the SIP URI is SIPS.
  - **udp**
    Specifies that the monitor uses UDP to communicate with the target.
- **name**
  Specifies a unique name for the component. This option is required for the commands **create**, **delete**, and **modify**.
- **partition**
  Displays the administrative partition within which the component resides.
- **probe-timeout**
  Specifies the number of seconds after which the BIG-IP® system times out the probe request to the BIG-IP system. The default value is **5** seconds.
- **regex**
  Displays the items that match the regular expression. The regular expression must be preceded by an at sign (@[regular expression]) to indicate that the identifier is a regular expression. See **help regex** for a description of regular expression syntax.
- **request**
  Specifies the SIP request line in the SIP message that is sent to the target. The default value is **none**.
- **timeout**
  Specifies the number of seconds the target has in which to respond to the monitor request. The default value is **120** seconds.
  If the target responds within the set time period, it is considered **up**. If the target does not respond within the set time period, it is considered **down**.

Also, if the target responds with a RESET packet, the system immediately flags the target as **down** without waiting for the timeout interval to expire.

See Also

create, *delete*, *edit*, glob, *pool*, *list*, *modify*, regex, *show*, *tmsh*

smtp

Configures a Simple Mail Transport Protocol (SMTP) monitor.

Syntax

Configure the **smtp** component within the **gtm monitor** module using the syntax in the following sections.

Create/Modify

```
create smtp [name]
modify smtp [name]
    debug [no | yes]
    defaults-from [name]
    description [string]
    destination [ip address][port]
    domain [ [name] | none]
    ignore-down-response [enabled | disabled]
    interval [integer]
    probe-timeout [integer]
    timeout [integer]
edit smtp [ [ [name] | [glob] | [regex] ] ... ]
    all-properties
    non-default-properties
```

Display

```
list smtp
list smtp [ [ [name] | [glob] | [regex] ] ... ]
show running-config smtp
show running-config smtp [ [ [name] | [glob] | [regex] ] ... ]
    all-properties
    non-default-properties
    one-line
    partition
```

Delete

```
delete smtp [name]
```

◆ Note

You cannot delete default monitors.

Description

You can use the **smtp** component to configure a custom monitor, or you can use the default SMTP monitor that the Global Traffic Manager provides. This type of monitor checks the status of a pool, pool member, or virtual server by issuing standard SMTP commands.

Examples

create smtp my_smtp defaults-from smtp

Creates a monitor named **my_smtp** that inherits properties from the default SMTP monitor.

list smtp

Displays the properties of all of the SMTP monitors.

Options

- **debug**
  Specifies whether the monitor sends error messages and additional information to a log file created and labeled specifically for this monitor. You can use the log information to help diagnose and troubleshoot unsuccessful health checks. The default value is **no**.
  The options are:
  - **no**
    Specifies that the system does not redirect error messages and additional information related to this monitor.
  - **yes**
    Specifies that the system redirects error messages and additional information to the /var/log/monitors/<monitor_name>-<node_name>-<port>.log file.
- **defaults-from**
  Specifies the name of the monitor from which you want your custom monitor to inherit settings. The default value is **smtp**.
- **description**
  User defined description.
- **destination**
  Specifies the IP address and service port of the resource that is the destination of this monitor. The default value is ***:***.
  Possible values are:
  - ***:***
    Specifies to perform a health check on the IP address and port supplied by a pool member.
  - ***:port**
    Specifies to perform a health check on the server with the IP address supplied by the pool member and the port you specify.
  - **IP address:port**
    Specifies to mark a pool member **up** or **down** based on the response of the server at the IP address and port you specify.
- **domain**
  Specifies the domain name to check, for example, **bigipinternal.com**. The default value is **none**.

- **glob**
  Displays the items that match the **glob** expression. See **help glob** for a description of **glob** expression syntax.
- **ignore-down-response**
  Specifies whether the monitor ignores a down response from the system it is monitoring. The default value is **disabled**.
- **interval**
  Specifies the frequency at which the system issues the monitor check. The default value is **30** seconds.
- **name**
  Specifies a unique name for the component. This option is required for the commands **create**, **delete**, and **modify**.
- **partition**
  Displays the administrative partition within which the component resides.
- **probe-timeout**
  Specifies the number of seconds after which the BIG-IP® system times out the probe request to the BIG-IP system. The default value is **5** seconds.
- **regex**
  Displays the items that match the regular expression. The regular expression must be preceded by an at sign (@[regular expression]) to indicate that the identifier is a regular expression. See **help regex** for a description of regular expression syntax.
- **timeout**
  Specifies the number of seconds the target has in which to respond to the monitor request. The default value is **120** seconds.
  If the target responds within the set time period, it is considered **up**. If the target does not respond within the set time period, it is considered **down**. Also, if the target responds with a RESET packet, the system immediately flags the target as **down** without waiting for the timeout interval to expire.

See Also

create, *delete*, *edit*, glob, *pool*, *list*, *modify*, regex, *show*, *tmsh*

snmp

Configures a Simple Network Management Protocol (SNMP) monitor.

Syntax

Configure the **snmp** component within the **gtm monitor** module using the syntax in the following sections.

Create/Modify

```
create snmp [name]
modify snmp [name]
    app-service [[string] | none]
    community [ [name] | none]
    defaults-from [name]
    description [string]
    destination [ip address] [port]
    ignore-down-response [enabled | disabled]
    interval [integer]
    port [integer]
    probe attempts [integer]
    probe-interval [integer]
    probe-timeout [integer]
    timeout [integer]
    version [ [integer] | none]
edit snmp [ [ [name] | [glob] | [regex] ] ... ]
    all-properties
    non-default-properties
```

Display

```
list snmp
list snmp [ [ [name] | [glob] | [regex] ] ... ]
show running-config snmp
show running-config snmp [ [ [name] | [glob] | [regex] ] ... ]
    all-properties
    non-default-properties
    one-line
    partition
```

Delete

```
delete snmp [name]
```

◆ Note

You cannot delete default monitors.

Description

You can use the **snmp** component to configure a custom monitor, or you can use the default SNMP monitor that the Global Traffic Manager provides. The SNMP monitor is both a health and performance monitor. This type of monitor checks the performance of a server running an SNMP agent such as UC Davis, for the purpose of load balancing traffic to that server.

Examples

create snmp my_snmp defaults-from snmp_gtm

Creates a monitor named **my_snmp** that inherits properties from the default SNMP monitor.

list snmp

Displays the properties of all of the SNMP monitors.

Options

- **app-service**
  Specifies the name of the application service to which the monitor belongs. The default value is **none**. **Note:** If the **strict-updates** option is **enabled** on the application service that owns the object, you cannot modify or delete the monitor. Only the application service can modify or delete the monitor.
- **community**
  Specifies the community name that the BIG-IP® system must use to authenticate with the host server through SNMP. The default value is **public**.
- **defaults-from**
  Specifies the name of the monitor from which you want your custom monitor to inherit settings. The default value is **snmp_gtm**.
- **description**
  User defined description.
- **destination**
  Specifies the IP address and service port of the resource that is the destination of this monitor. The default value is ***:***.
  Possible values are:
  - ***:***
    Specifies to perform a health check on the IP address and port supplied by a pool member.
  - ***:port**
    Specifies to perform a health check on the server with the IP address supplied by the pool member and the port you specify.
  - **IP address:port**
    Specifies to mark a pool member **up** or **down** based on the response of the server at the IP address and port you specify.

- **glob**
  Displays the items that match the **glob** expression. See **help glob** for a description of **glob** expression syntax.
- **ignore-down-response**
  Specifies whether the monitor ignores a down response from the system it is monitoring. The default value is **disabled**.
- **interval**
  Specifies the frequency at which the system issues the monitor check. The default value is **90** seconds.
- **name**
  Specifies a unique name for the component. This option is required for the commands **create**, **delete**, and **modify**.
- **partition**
  Displays the administrative partition within which the component resides.
- **port**
  Specifies the port number to which this monitor sends SNMP traps. The default value is **161**.
- **probe-attempts**
  Specifies the number of times the BIG-IP system attempts to probe the host server, after which the BIG-IP system considers the host server down or unavailable. The default value is **1**.
- **probe-interval**
  Specifies the frequency at which the BIG-IP system probes the host server. The default value is **1**.
- **probe-timeout**
  Specifies the number of seconds after which the BIG-IP system times out the probe request to the BIG-IP system. The default value is **5** seconds.
- **regex**
  Displays the items that match the regular expression. The regular expression must be preceded by an at sign (@[regular expression]) to indicate that the identifier is a regular expression. See **help regex** for a description of regular expression syntax.
- **timeout**
  Specifies the number of seconds the target has in which to respond to the monitor request. The default value is **180** seconds.
  If the target responds within the set time period, it is considered **up**. If the target does not respond within the set time period, it is considered **down**. Also, if the target responds with a RESET packet, the system immediately flags the target as **down** without waiting for the timeout interval to expire.
- **version**
  Specifies the SNMP version the monitor uses. The default value is **v1**.

See Also

create, *delete*, *edit*, glob, *pool*, *list*, *modify*, regex, *show*, *tmsh*

snmp-link

Configures a Simple Network Management Protocol (SNMP) link monitor.

Syntax

Configure the **snmp-link** component within the **gtm monitor** module using the syntax in the following sections.

Create/Modify

```
create snmp-link [name]
modify snmp-link [name]
    app-service [[string] | none]
    community [[name] | none]
    defaults-from [name]
    description [string]
    destination [ip address]
    ignore-down-response [enabled | disabled]
    interval [integer]
    port [ [integer] | none]
    probe attempts [integer]
    probe-interval [integer]
    probe-timeout [integer]
    timeout [integer]
    version [ [integer] | none]
edit snmp-link [ [ [name] | [glob] | [regex] ] ... ]
    all-properties
    non-default-properties
```

Display

```
list snmp-link
list snmp-link [ [ [name] | [glob] | [regex] ] ... ]
show running-config snmp-link
show running-config snmp-link [ [ [name] | [glob] | [regex] ] ... ]
    all-properties
    non-default-properties
    one-line
    partition
```

Delete

```
delete snmp-link [name]
```

◆ Note

You cannot delete default monitors.

Description

You can use the **snmp-link** component to configure a custom monitor, or you can use the default SNMP Link monitor that the Global Traffic Manager provides. This type of monitor checks the current CPU, memory, and disk usage of a pool, pool member, or virtual server that is running an SNMP data collection agent, and then dynamically load balances traffic accordingly.

Examples

create snmp-link my_snmp-link defaults-from snmp_link

Creates a monitor named **my_snmp-link** that inherits properties from the default SNMP Link monitor.

list snmp-link

Displays the properties of all of the SNMP Link monitors.

Options

- **app-service**
  Specifies the name of the application service to which the monitor belongs. The default value is **none**. **Note:** If the **strict-updates** option is **enabled** on the application service that owns the object, you cannot modify or delete the monitor. Only the application service can modify or delete the monitor.
- **community**
  Specifies the community name that the BIG-IP® system must use to authenticate with the host server through SNMP. The default value is **public**.
- **defaults-from**
  Specifies the name of the monitor from which you want your custom monitor to inherit settings. The default value is **snmp_link**.
- **description**
  User defined description.
- **destination**
  Specifies the IP address of the resource that is the destination of this monitor. The default value is *****.
  Possible values are:
  - *****
    Specifies to perform a health check on the IP address of the node.
  - **IP address**
    Specifies to perform a health check on the IP address that you specify, route the check through the IP address of the associated node, and mark the IP address of the associated node **up** or **down** accordingly.

- **glob**
  Displays the items that match the **glob** expression. See **help glob** for a description of **glob** expression syntax.
- **ignore-down-response**
  Specifies whether the monitor ignores a down response from the system it is monitoring. The default value is **disabled**.
- **interval**
  Specifies the frequency at which the system issues the monitor check. The default value is **10** seconds.
- **name**
  Specifies a unique name for the component. This option is required for the commands **create**, **delete**, and **modify**.
- **partition**
  Displays the administrative partition within which the component resides.
- **port**
  Specifies the port number to which this monitor sends SNMP traps. The default value is **161**.
- **probe-attempts**
  Specifies the number of times the BIG-IP system attempts to probe the host server, after which the BIG-IP system considers the host server down or unavailable. The default value is **3**.
- **probe-interval**
  Specifies the frequency at which the BIG-IP system probes the host server. The default value is **0**.
- **probe-timeout**
  Specifies the number of seconds after which the BIG-IP system times out the probe request to the BIG-IP system. The default value is **5** seconds.
- **regex**
  Displays the items that match the regular expression. The regular expression must be preceded by an at sign (@[regular expression]) to indicate that the identifier is a regular expression. See **help regex** for a description of regular expression syntax.
- **timeout**
  Specifies the number of seconds the target has in which to respond to the monitor request. The default value is **30** seconds.
  If the target responds within the set time period, it is considered **up**. If the target does not respond within the set time period, it is considered **down**. Also, if the target responds with a RESET packet, the system immediately flags the target as **down** without waiting for the timeout interval to expire.
- **version**
  Specifies the SNMP version the monitor uses. The default value is **none**.

See Also

create, *delete*, *edit*, glob, *list*, *node*, *modify*, regex, *show*, *tmsh*

soap

Configures a Simple Object Access Protocol (SOAP) monitor.

Syntax

Configure the **soap** component within the **gtm monitor** module using the syntax in the following sections.

Create/Modify

```
create soap [name]
modify soap [name]
    debug [no | yes]
    defaults-from [name]
    description [string]
    destination [ip address][port]
    expect-fault [no | yes]
    ignore-down-response [enabled | disabled]
    interval [integer]
    method [string]
    namespace [ [name] | none]
    parameter-name [ [name] | none]
    parameter-type [bool | int | long | [string] ]
    parameter-value [none | [integer] | [string] ]
    password [none | [password] ]
    probe-timeout [integer]
    protocol [[none] | [protocol] ]
    return-type [bool | char | double | int | long | short | [string] ]
    return-value [none | [integer] | [string] ]
    soap-action [string]
    timeout [integer]
    url-path [none | [string] ]
    username [ [name] | none]
edit soap [ [ [name] | [glob] | [regex] ] ... ]
    all-properties
    non-default-properties
```

Display

```
list soap
list soap [ [ [name] | [glob] | [regex] ] ... ]
show running-config soap
show running-config soap [ [ [name] | [glob] | [regex] ] ... ]
    all-properties
    non-default-properties
    one-line
    partition
```

Delete

```
delete soap [name]
```

◆ Note

You cannot delete default monitors.

Description

You can use the **soap** component to configure a custom monitor, or you can use the default SOAP monitor that the Global Traffic Manager provides. This type of monitor tests a Web service based on SOAP.

Examples

create soap my_soap defaults-from soap

Creates a monitor named **my_soap** that inherits values from the system default SOAP monitor.

list soap

Displays the properties of all of the SOAP monitors.

Options

- **debug**
  Specifies whether the monitor sends error messages and additional information to a log file created and labeled specifically for this monitor. You can use the log information to help diagnose and troubleshoot unsuccessful health checks. The default value is **no**.
  The options are:
  - **no**
    Specifies that the system does not redirect error messages and additional information related to this monitor.
  - **yes**
    Specifies that the system redirects error messages and additional information to the /var/log/monitors/<monitor_name>-<node_name>-<port>.log file.
- **defaults-from**
  Specifies the type of monitor you want to use to create the new monitor. The default value is **soap**.
- **description**
  User defined description.
- **destination**
  Specifies the IP address and service port of the resource that is the destination of this monitor. Possible values are:

- ***:***
  Specifies to perform a health check on the IP address and port supplied by a pool member.
- ***:port**
  Specifies to perform a health check on the server with the IP address supplied by the pool member and the port you specify.
- **IP address:port**
  Specifies to mark a pool member **up** or **down** based on the response of the server at the IP address and port you specify.

◆ **expect-fault**
Specifies whether the value of the **method** option causes the monitor to expect a SOAP fault message. The default value is **no**.

◆ **glob**
Displays the items that match the **glob** expression. See **help glob** for a description of **glob** expression syntax.

◆ **ignore-down-response**
Specifies whether the monitor ignores a down response from the system it is monitoring. The default value is **disabled**.

◆ **interval**
Specifies the frequency at which the system issues the monitor check. The default value is **30** seconds.

◆ **method**
Specifies the method by which the monitor contacts the resource.

◆ **name**
Specifies a unique name for the component. This option is required for the commands **create**, **delete**, and **modify**.

◆ **namespace**
Specifies the name space for the Web service you are monitoring, for example, **http://example.com/**. The default value is **none**.

◆ **parameter-name**
If the method has a parameter, specifies the name of that parameter. The default value is **bool**.

◆ **parameter-type**
Specifies the parameter type. The default value is **none**.

◆ **parameter-value**
Specifies the value for the parameter. The default value is **none**.

◆ **partition**
Displays the administrative partition within which the component resides.

◆ **password**
Specifies the password if the monitored target requires authentication. The default value is **none**.

◆ **probe-timeout**
Specifies the number of seconds after which the BIG-IP® system times out the probe request to the BIG-IP system. The default value is **5** seconds.

- **protocol**
  Specifies the protocol that the monitor uses to communicate with the target. The default value is **none**.
- **regex**
  Displays the items that match the regular expression. The regular expression must be preceded by an at sign (@[regular expression]) to indicate that the identifier is a regular expression. See **help regex** for a description of regular expression syntax.
- **return-type**
  Specifies the type for the returned parameter. The default value is **bool**.
- **return-value**
  Specifies the value for the returned parameter. The default value is **none**.
- **soap-action**
  Specifies the value for the SOAPAction header. The default value is the empty string.
- **timeout**
  Specifies the number of seconds the target has in which to respond to the monitor request. The default value is **120** seconds. If the target responds within the set time period, it is considered up. If the target does not respond within the set time period, it is considered down. Also, if the target responds with a RESET packet, the system immediately flags the target as down without waiting for the timeout interval to expire.
- **url-path**
  Specifies the URL for the Web service that you are monitoring, for example, **/services/myservice.aspx**. The default value is **none**.
- **username**
  Specifies the user name if the monitored target requires authentication. The default value is **none**.

See Also

create, *delete*, *edit*, glob, *pool*, *list*, *modify*, regex, *show*, *tmsh*

tcp

Configures a Transmission Control Protocol (TCP) monitor.

Syntax

Configure the **tcp** component within the **gtm monitor** module using the syntax in the following sections.

Create/Modify

```
create tcp [name]
modify tcp [name]
    defaults-from [name]
    description [string]
    destination [ip address][port]
    ignore-down-response [enabled | disabled]
    interval [integer]
    probe-timeout [integer]
    recv [none | [string] ]
    reverse [enabled | disabled]
    send [none | [string] ]
    timeout [integer]
    transparent [disabled | enabled]
edit tcp [ [ [name] | [glob] | [regex] ] ... ]
    all-properties
    non-default-properties
```

Display

```
list tcp
list tcp [ [ [name] | [glob] | [regex] ] ... ]
show running-config tcp
show running-config tcp [ [ [name] | [glob] | [regex] ] ... ]
    all-properties
    non-default-properties
    one-line
    partition
```

Delete

```
delete tcp [name]
```

◆ Note

You cannot delete default monitors.

Description

You can use the **tcp** component to configure a custom monitor, or you can use the default TCP monitor that the Global Traffic Manager provides.

Examples

create tcp my_tcp defaults-from tcp

Creates a monitor named **my_tcp** that inherits properties from the default TCP monitor.

list tcp

Displays the properties of all of the TCP monitors.

Options

- **defaults-from**
  Specifies the name of the monitor from which you want your custom monitor to inherit settings. The default value is **tcp**.
- **description**
  User defined description.
- **destination**
  Specifies the IP address and service port of the resource that is the destination of this monitor. The default value is ***:***.
  Possible values are:
  - ***:***
    Specifies to perform a health check on the IP address and port supplied by a pool member.
  - ***:port**
    Specifies to perform a health check on the server with the IP address supplied by the pool member and the port you specify.
  - **IP address:port**
    Specifies to mark a pool member **up** or **down** based on the response of the server at the IP address and port you specify.
  - **IP address:port** (with the **transparent** option **enabled**)
    Specifies to perform a health check on the server at the IP address and port you specify, route the check through the IP address and port supplied by the pool member, and mark the pool member (the gateway) **up** or **down** accordingly.
- **glob**
  Displays the items that match the **glob** expression. See **help glob** for a description of **glob** expression syntax.
- **ignore-down-response**
  Specifies whether the monitor ignores a down response from the system it is monitoring. The default value is **disabled**.
- **interval**
  Specifies the frequency at which the system issues the monitor check. The default value is **30** seconds.
- **name**
  Specifies a unique name for the component. This option is required for the commands **create**, **delete**, and **modify**.

- **partition**
  Displays the administrative partition within which the component resides.
- **probe-timeout**
  Specifies the number of seconds after which the BIG-IP® system times out the probe request to the BIG-IP system. The default value is **5** seconds.
- **recv**
  Specifies the text string that the monitor looks for in the returned resource. The default value is **none**.
  The most common receive expressions contain a text string that is included in an HTML file on your site. The text string can be regular text, HTML tags, or image names. If you do not specify a value for both the **send** and **recv** options, the monitor performs a simple service check and connect only.
- **regex**
  Displays the items that match the regular expression. The regular expression must be preceded by an at sign (@[regular expression]) to indicate that the identifier is a regular expression. See **help regex** for a description of regular expression syntax.
- **reverse**
  Specifies whether the monitor operates in reverse mode. When the monitor is in reverse mode, a successful check marks the monitored object **down** instead of **up**. You can use the this mode only if you configure both the **send** and **recv** options.
  The default value is **disabled**, which specifies that the monitor does not operate in reverse mode. The **enabled** value specifies that the monitor operates in reverse mode.
- **send**
  Specifies the text string that the monitor sends to the target object. The default setting is **GET /**, which retrieves a default HTML file for a web site.
  To retrieve a specific page from a web site, specify a fully-qualified path name, for example, **GET /www/company/index.html**. Since the string may have special characters, the system may require that the string be enclosed with single quotation marks.
  If this value is null, then a valid connection suffices to determine that the service is **up**. In this case, the system does not need the recv option and ignores the option even if not null.
- **timeout**
  Specifies the number of seconds the target has in which to respond to the monitor request. The default value is **120** seconds.
  If the target responds within the set time period, it is considered **up**. If the target does not respond within the set time period, it is considered **down**. Also, if the target responds with a RESET packet, the system immediately flags the target as **down** without waiting for the timeout interval to expire.

- **transparent**
  Specifies whether the monitor operates in transparent mode. Monitors in transparent mode can monitor pool members through firewalls. The default value is **disabled**.

See Also

create, *delete*, *edit*, glob, *pool*, *server*, *list*, *modify*, regex, *show*, *tmsh*

tcp-half-open

Configures a Transmission Control Protocol (TCP) Half Open monitor.

Syntax

Configure the **tcp-half-open** component within the **gtm monitor** module using the syntax in the following sections.

Create/Modify

```
create tcp-half-open [name]
modify tcp-half-open [name]
    defaults-from [name]
    description [string]
    destination [ip address][port]
    ignore-down-response [enabled | disabled]
    interval [integer]
    probe-attempts [integer])
    probe-interval [integer])
    probe-timeout [integer]
    timeout [integer]
    transparent [disabled | enabled]
edit tcp-half-open [ [ [name] | [glob] | [regex] ] ... ]
    all-properties
    non-default-properties
```

Display

```
list tcp-half-open
list tcp-half-open [ [ [name] | [glob] | [regex] ] ... ]
show running-config tcp-half-open
show running-config tcp-half-open [ [ [name] | [glob] | [regex] ] ... ]
    all-properties
    non-default-properties
    one-line
    partition
```

Delete

```
delete tcp-half-open [name]
```

◆ Note

You cannot delete default monitors.

Description

You can use the **tcp-half-open** component to configure a custom monitor, or you can use the default TCP Half Open monitor that the Global Traffic Manager provides.

For more information about configuring monitors, refer to the Configuration Guide for BIG-IP® Global Traffic Management.

Examples

create tcp-half-open my_tcp-half-open defaults-from tcp_half_open

Creates a monitor named **my_tcp-half-open** that inherits properties from the default TCP Half Open monitor.

list tcp-half-open

Displays the properties of all of the TCP Half Open monitors.

Options

- **defaults-from**
  Specifies the name of the monitor from which you want your custom monitor to inherit settings. The default value is **tcp_half_open**.
- **description**
  User defined description.
- **destination**
  Specifies the IP address and service port of the resource that is the destination of this monitor. The default value is ***:***.
  Possible values are:
  - ***:***
    Specifies to perform a health check on the IP address and port supplied by a pool member.
  - ***:port**
    Specifies to perform a health check on the server with the IP address supplied by the pool member and the port you specify.
  - **IP address:port**
    Specifies to mark a pool member **up** or **down** based on the response of the server at the IP address and port you specify.
  - **IP address:port** (with the **transparent** option **enabled**)
    Specifies to perform a health check on the server at the IP address and port you specify, route the check through the IP address and port supplied by the pool member, and mark the pool member (the gateway) **up** or **down** accordingly.
- **glob**
  Displays the items that match the **glob** expression. See **help glob** for a description of **glob** expression syntax.
- **ignore-down-response**
  Specifies whether the monitor ignores a down response from the system it is monitoring. The default value is **disabled**.
- **interval**
  Specifies the frequency at which the system issues the monitor check. The default value is **30** seconds.

- **name**
  Specifies a unique name for the component. This option is required for the commands **create**, **delete**, and **modify**.
- **partition**
  Displays the administrative partition within which the component resides.
- **probe-attempts**
  Specifies the number of times the BIG-IP system attempts to probe the host server, after which the BIG-IP system considers the host server down or unavailable. The default value is **3**.
- **probe-interval**
  Specifies the frequency at which the BIG-IP system probes the host server. The default value is **1**.
- **probe-timeout**
  Specifies the number of seconds after which the BIG-IP system times out the probe request to the BIG-IP system. The default value is **5** seconds.
- **regex**
  Displays the items that match the regular expression. The regular expression must be preceded by an at sign (@[regular expression]) to indicate that the identifier is a regular expression. See **help regex** for a description of regular expression syntax.
- **timeout**
  Specifies the number of seconds the target has in which to respond to the monitor request. The default value is **120** seconds.
  If the target responds within the set time period, it is considered **up**. If the target does not respond within the set time period, it is considered **down**. Also, if the target responds with a RESET packet, the system immediately flags the target as **down** without waiting for the timeout interval to expire.
- **transparent**
  Specifies whether the monitor operates in transparent mode. Monitors in transparent mode can monitor pool members through firewalls. The default value is **disabled**.

See Also

create, *delete*, *edit*, glob, *pool*, *server*, *list*, *modify*, regex, *show*, *tmsh*

udp

Configures a User Datagram Protocol (UDP) monitor.

Syntax

Configure the **udp** component within the **gtm monitor** module using the syntax in the following sections.

Create/Modify

```
create udp [name]
modify udp [name]
    debug [no | yes]
    defaults-from [name]
    description [string]
    destination [ip address][port]
    ignore-down-response [enabled | disabled]
    interval [integer]
    probe-attempts [integer]
    probe-interval [integer]
    probe-timeout [integer]
    reverse [enabled | disabled]
    send [none | [string] ]
    timeout [integer]
    transparent [disabled | enabled]
edit udp [ [ [name] | [glob] | [regex] ] ... ]
    all-properties
    non-default-properties
```

Display

```
list udp
list udp [ [ [name] | [glob] | [regex] ] ... ]
show running-config udp
show running-config udp [ [ [name] | [glob] | [regex] ] ... ]
    all-properties
    non-default-properties
    one-line
    partition
```

Delete

```
delete udp [name]
```

◆ Note

You cannot delete default monitors.

Description

You can use the **udp** component to configure a custom monitor, or you can use the default UDP monitor that the Global Traffic Manager provides. This type of monitor verifies the UDP service by attempting to send UDP packets to a pool, pool member, or virtual server, and receiving a reply.

For more information about configuring monitors, refer to the Configuration Guide for BIG-IP® Global Traffic Management.

Examples

create udp my_udp defaults-from udp

Creates a monitor named **my_udp** that inherits properties from the default UDP monitor.

list udp

Displays the properties of all of the UDP monitors.

Options

- **debug**
  Specifies whether the monitor sends error messages and additional information to a log file created and labeled specifically for this monitor. You can use the log information to help diagnose and troubleshoot unsuccessful health checks. The default value is **no**.
  The options are:
  - **no**
    Specifies that the system does not redirect error messages and additional information related to this monitor.
  - **yes**
    Specifies that the system redirects error messages and additional information to the /var/log/monitors/<monitor_name>-<node_name>-<port>.log file.
- **defaults-from**
  Specifies the name of the monitor from which you want your custom monitor to inherit settings. The default value is **udp**.
- **description**
  User defined description.
- **destination**
  Specifies the IP address and service port of the resource that is the destination of this monitor. Possible values are:
  - ***:***
    Specifies to perform a health check on the IP address and port supplied by a pool member.

- ***:port**
  Specifies to perform a health check on the server with the IP address supplied by the pool member and the port you specify.
- **IP address:port**
  Specifies to mark a pool member **up** or **down** based on the response of the server at the IP address and port you specify.
- **IP address:port** (with the **transparent** option **enabled**)
  Specifies to perform a health check on the server at the IP address and port you specify, route the check through the IP address and port supplied by the pool member, and mark the pool member (the gateway) **up** or **down** accordingly.

◆ **glob**
Displays the items that match the **glob** expression. See **help glob** for a description of **glob** expression syntax.

◆ **ignore-down-response**
Specifies whether the monitor ignores a down response from the system it is monitoring. The default value is **disabled**.

◆ **interval**
Specifies the frequency at which the system issues the monitor check. The default value is **30** seconds.

◆ **name**
Specifies a unique name for the component. This option is required for the commands **create**, **delete**, and **modify**.

◆ **partition**
Displays the administrative partition within which the component resides.

◆ **probe-attempts**
Specifies the number of times the BIG-IP system attempts to probe the host server, after which the BIG-IP system considers the host server down or unavailable. The default value is **3**.

◆ **probe-interval**
Specifies the frequency at which the BIG-IP system probes the host server. The default value is **1**.

◆ **probe-timeout**
Specifies the number of seconds after which the BIG-IP system times out the probe request to the BIG-IP system. The default value is **5** seconds.

◆ **regex**
Displays the items that match the regular expression. The regular expression must be preceded by an at sign (@[regular expression]) to indicate that the identifier is a regular expression. See **help regex** for a description of regular expression syntax.

◆ **reverse**
Specifies whether the monitor operates in reverse mode. When the monitor is in reverse mode, a successful check marks the monitored object **down** instead of **up**.

The default value is **disabled**, which specifies that the monitor does not operate in reverse mode. The **enabled** value specifies that the monitor operates in reverse mode.

- **send**
  Specifies the text string that the monitor sends to the target object. The default value is "default send string".
  To retrieve a specific page from a web site, specify a fully-qualified path name, for example, **GET /www/company/index.html**. Since the string may have special characters, the system may require that the string be enclosed with single quotation marks.
  If this value is null, then a valid connection suffices to determine that the service is up. In this case, the system does not need the value of the **recv** option and ignores the option even if not null.
- **timeout**
  Specifies the number of seconds the target has in which to respond to the monitor request. The default value is **120** seconds. If the target responds within the set time period, it is considered up. If the target does not respond within the set time period, it is considered down. Also, if the target responds with a RESET packet, the system immediately flags the target as down without waiting for the timeout interval to expire.
- **transparent**
  Specifies whether the monitor operates in transparent mode. Monitors in transparent mode can monitor pool members through firewalls. The default value is **disabled**.

See Also

create, *delete*, *edit*, glob, *pool*, *server*, *list*, *modify*, regex, *show*, *tmsh*

wap

Configures a Wireless Application Protocol (WAP) monitor.

Syntax

Configure the **wap** component within the **gtm monitor** module using the syntax in the following sections.

Create/Modify

```
create wap [name]
modify wap [name]
    accounting-node [none | [RADIUS server name] ]
    accounting-port [ [integer] | none]
    call-id [none | [RADIUS server 11 digit phone number] ]
    check-until-up [enabled | disabled]
    debug [no | yes]
    defaults-from [name]
    description [string]
    destination [ip address][port]
    framed-address [none | [RADIUS framed IP address] ]
    ignore-down-response [enabled | disabled]
    interval [integer]
    probe-timeout [integer]
    recv [none | [string] ]
    secret [none | [password] ]
    send [none | [string] ]
    server-id [none | [RADIUS NAS-ID] ]
    session-id [none | [RADIUS session ID] ]
    timeout [integer]
edit wap [ [ [name] | [glob] | [regex] ] ... ]
    all-properties
    non-default-properties
```

Display

```
list wap
list wap[ [ [name] | [glob] | [regex] ] ... ]
show running-config wap
show running-config wap[ [ [name] | [glob] | [regex] ] ... ]
    all-properties
    non-default-properties
    one-line
    partition
```

Delete

```
delete wap [name]
```

◆ Note

You cannot delete default monitors.

Description

You can use the **wap** component to configure a custom monitor, or you can use the default WAP monitor that the Global Traffic Manager provides. This type of monitor requests the URL specified in the **send** option, and finds the string specified in the **recv** option somewhere in the data returned by the URL response.

Examples

create wap my_wap defaults-from wap

Creates a monitor named **my_wap** that inherits properties from the default WAP monitor.

list wap

Displays the properties of all of the WAP monitors.

Options

- **accounting-node**
  Specifies the RADIUS server that provides authentication for the WAP target. Note that if you configure the **accounting-port** option, but you do not configure the this option, the system assumes that the RADIUS server and the WAP server are the same system.
- **accounting-port**
  Specifies the port that the monitor uses for RADIUS accounting. The default value is **none**. A value of **0** (zero) disables RADIUS accounting.
- **call-id**
  Specifies the 11-digit phone number for the RADIUS server. The default value is **none**.
- **debug**
  Specifies whether the monitor sends error messages and additional information to a log file created and labeled specifically for this monitor. You can use the log information to help diagnose and troubleshoot unsuccessful health checks. The default value is **no**.
  The options are:
  - **no**
    Specifies that the system does not redirect error messages and additional information related to this monitor.
  - **yes**
    Specifies that the system redirects error messages and additional information to the /var/log/monitors/<monitor_name>-<node_name>-<port>.log file.
- **defaults-from**
  Specifies the name of the monitor from which you want your custom monitor to inherit settings. The default value is **wap**.

- **description**
  User defined description.
- **destination**
  Specifies the IP address and service port of the resource that is the destination of this monitor. The default value is ***:***.
  Possible values are:
  - ***:***
    Specifies to perform a health check on the IP address and port supplied by a pool member.
  - ***:port**
    Specifies to perform a health check on the server with the IP address supplied by the pool member and the port you specify.
  - **IP address:port**
    Specifies to mark a pool member **up** or **down** based on the response of the server at the IP address and port you specify.
- **framed-address**
  Specifies the RADIUS framed IP address. The default value is **none**.
- **glob**
  Displays the items that match the **glob** expression. See **help glob** for a description of **glob** expression syntax.
- **ignore-down-response**
  Specifies whether the monitor ignores a down response from the system it is monitoring. The default value is **disabled**.
- **interval**
  Specifies the frequency at which the system issues the monitor check. The default value is **10** seconds.
- **name**
  Specifies a unique name for the component. This option is required for the commands **create**, **delete**, and **modify**.
- **partition**
  Displays the administrative partition within which the component resides.
- **probe-timeout**
  Specifies the number of seconds after which the BIG-IP® system times out the probe request to the BIG-IP system. The default value is **5** seconds.
- **recv**
  Specifies the text string that the monitor looks for in the returned resource. The most common receive expressions contain a text string that is included in an HTML file on your site. The text string can be regular text, HTML tags, or image names. If you do not specify both a value for both the **send** and **recv** options, the monitor performs a simple service check and connect only. The default value is **none**.

- **regex**
  Displays the items that match the regular expression. The regular expression must be preceded by an at sign (@[regular expression]) to indicate that the identifier is a regular expression. See **help regex** for a description of regular expression syntax.
- **secret**
  Specifies the password the monitor needs to communicate with the resource. The default value is **none**.
- **send**
  Specifies the text string that the monitor sends to the target object. The default setting is **GET /**, which retrieves a default HTML file for a web site.
  To retrieve a specific page from a web site, specify a fully-qualified path name, for example, **GET /www/company/index.html**. Since the string may have special characters, the system may require that the string be enclosed with single quotation marks.
  If this value is null, then a valid connection suffices to determine that the service is up. In this case, the system does not need the recv option and ignores the option even if it is not null. The default value is **none**.
- **server-id**
  Specifies the RADIUS NAS-ID for this system when configuring a RADIUS server. The default value is **none**.
- **session-id**
  Specifies the RADIUS session identification number when configuring a RADIUS server. The default value is **none**.
- **timeout**
  Specifies the number of seconds the target has in which to respond to the monitor request. The default value is **31** seconds.
  If the target responds within the set time period, it is considered **up**. If the target does not respond within the set time period, it is considered **down**. Also, if the target responds with a RESET packet, the system immediately flags the target as **down** without waiting for the timeout interval to expire.

See Also

create, *delete*, *edit*, glob, *pool*, *list*, *modify*, regex, *show*, *tmsh*

wmi

Configures a Windows® Management Instrumentation (WMI) monitor.

Syntax

Configure the **wmi** component within the **gtm monitor** module using the syntax in the following sections.

Create/Modify

```
create wmi [name]
modify wmi [name]
    command [[command] | none]
    defaults-from [name]
    description [string]
    ignore-down-response [enabled | disabled]
    interval [integer]
    metrics [ [integer] | none]
    password [none | [password] ]
    probe-timeout [integer]
    timeout [integer]
    url [none | [URL]]
    username [ [name] | none]
edit wmi [ [ [name] | [glob] | [regex] ] ... ]
    all-properties
    non-default-properties
```

Display

```
list wmi
list wmi [ [ [name] | [glob] | [regex] ] ... ]
show running-config wmi
show running-config wmi [ [ [name] | [glob] | [regex] ] ... ]
    agent
    all-properties
    method
    non-default-properties
    one-line
    partition
    post
```

Delete

```
delete wmi [name]
```

◆ Note

You cannot delete default monitors.

Description

You can use the **wmi** component to configure a custom monitor, or you can use the default WMI monitor that the Global Traffic Manager provides. This type of monitor checks the performance of a pool, pool member, or virtual server that is running the WMI data collection agent, and then dynamically load balances traffic accordingly.

Examples

create wmi my_wmi defaults-from wmi

Creates a monitor named **my_wmi** that inherits properties from the default WMI monitor.

list wmi

Displays the properties of all of the WMI monitors.

Options

- **agent**
  Displays the agent for the monitor. The default agent is **Mozilla/4.0 (compatible: MSIE 5.0; Windows NT)**. You cannot modify the agent.
- **command**
  Specifies the command that the system uses to obtain the metrics from the resource. See the documentation for this resource for information on available commands.
- **defaults-from**
  Specifies the name of the monitor from which you want your custom monitor to inherit settings. The default value is **wmi**.
- **description**
  User defined description.
- **glob**
  Displays the items that match the **glob** expression. See **help glob** for a description of **glob** expression syntax.
- **ignore-down-response**
  Specifies whether the monitor ignores a down response from the system it is monitoring. The default value is **disabled**.
- **interval**
  Specifies the frequency at which the system issues the monitor check. The default value is **30** seconds.
- **method**
  Displays the GET method. You cannot modify the method.
- **metrics**
  Specifies the performance metrics that the commands collect from the target. The default value is **LoadPercentage, DiskUsage, PhysicalMemoryUsage:1.5, VirtualMemoryUsage:2.0**.

- **name**
  Specifies a unique name for the component. This option is required for the commands **create**, **delete**, and **modify**.
- **partition**
  Displays the administrative partition within which the component resides.
- **password**
  Specifies the password if the monitored target requires authentication. The default value is **none**.
- **post**
  Specifies the mechanism that the monitor uses for posting. The default value is **RespFormat=HTML**. You cannot change the post format for WMI monitors.
- **probe-timeout**
  Specifies the number of seconds after which the BIG-IP® system times out the probe request to the BIG-IP system. The default value is **5** seconds.
- **regex**
  Displays the items that match the regular expression. The regular expression must be preceded by an at sign (@[regular expression]) to indicate that the identifier is a regular expression. See **help regex** for a description of regular expression syntax.
- **timeout**
  Specifies the number of seconds the target has in which to respond to the monitor request. The default value is **120** seconds.
  If the target responds within the set time period, it is considered **up**. If the target does not respond within the set time period, it is considered **down**. Also, if the target responds with a RESET packet, the system immediately flags the target as **down** without waiting for the timeout interval to expire.
- **url**
  Specifies the URL that the monitor uses. The default value is **/scripts/f5Isapi.dll**.
- **username**
  Specifies the user name if the monitored target requires authentication. The default value is **none**.

See Also

create, *delete*, *edit*, glob, *pool*, *list*, *node*, *modify*, regex, *show*, *tmsh*

49

ltm

- Introducing the ltm module
- Alphabetical list of components

Introducing the ltm module

You can use the tmsh components that reside within the ltm module to configure Local Traffic Manager™. For more information about the tmsh hierarchical structure, see Chapter 2, *Understanding and Using the Traffic Management Shell*.

Alphabetical list of components

The remainder of this chapter lists the tmsh components that are available in the ltm module.

alg-log-profile

Configures an Application-Level Gateway logging profile.

Syntax

Create/Modify

```
create alg-log-profile [name]
modify alg-log-profile [name | all]
    app-service [[string] | none]
    start-control-channel {
        action [disabled | enabled | backup-allocation-only]
        elements [add | delete | replace-all-with] {
            destination
        }
    }
    end-control-channel {
        action [disabled | enabled | backup-allocation-only]
        elements [add | delete | replace-all-with] {
            destination
        }
    }
    start-data-channel {
        action [disabled | enabled | backup-allocation-only]
        elements [add | delete | replace-all-with] {
            destination
        }
    }
    end-data-channel {
        action [disabled | enabled | backup-allocation-only]
        elements [add | delete | replace-all-with] {
            destination
        }
    }
    inbound-transaction {
        action [disabled | enabled]
    }
edit alg-log-profile [ [ [name] | [glob] | [regex] ] ... ]
    all-properties
    non-default-properties
reset-stats alg-log-profile
reset-stats alg-log-profile [ [ [name] | [glob] | [regex] ] ... ]
```

Display

```
list alg-log-profile
list alg-log-profile [ [ [name] | [glob] | [regex] ] ... ]
show running-config alg-log-profile
show running-config alg-log-profile [ [ [name] | [glob] | [regex] ] ... ]
    all-properties
    non-default-properties
    one-line
```

Delete

```
delete alg-log-profile [name | all]
```

Description

A ALG log profile allows fine grain control of the logging for ALG events. When attached to an supported ALG profile - currently FTP, RTSP, SIP, you can control the events to log as well as optional elements in the log entry.

Examples

create ltm alg-log-profile my_alg_log_profile end-control-channel { action backup-allocation-only } end-data-channel { action backup-allocation-only }

Creates the ALG log profile**my_alg_log_profile** that generates log entries for both inbound and data-channel when translation is from backup members only.

delete alg-log-profile my_lsn_log_profile

Deletes the ALG log profile named **my_lsn_log_profile**.

Options

- **app-service**
  Specifies the name of the application service to which this object belongs. The default value is **none**.

Note

*If the **strict-updates** option is **enabled** on the application service that owns the object, you cannot modify or delete this object. Only the application service can modify or delete this object.*

- **events**
  The type of ALG events available for logging control.
  - **start-control-channel**
    Event for start of control channel connection.
  - **end-control-channel**
    Event for end of control channel connection.
  - **start-data-channel**
    Event for start of data channel connection.
  - **end-data-channel**
    Event for end of data channel connection.

- **inbound-transaction**
  Event for inbound transaction event to an ALG end-point. Inbound transaction log entry could contain both incoming and outgoing messages.

◆ **action**
Specify the logging action to be taken when a particular event is encountered.

- **enabled**
  Logging is enable for the event, regardless of how the flow is created.
- **backup-allocation-only**
  Logging is enable for the event, when the ALG is proxy with a LSN, and translation is take from backup pool member only.
- **disabled**
  Logging is disable for the event.

◆ **elements**
Optional elements that can be added to the log message.

◆ **regex**
Displays the items that match the regular expression. The regular expression must be preceded by an at sign (@[regular expression]) to indicate that the identifier is a regular expression. See **help regex** for a description of regular expression syntax.

See Also

ftp, *sip*, *rtsp*, *create*, *delete*, *edit*, glob, *list*, *ltm*, *modify*, regex, *tmsh*

default-node-monitor

Configures the default node monitor for the Local Traffic Manager.

Syntax

Configure the **default-node-monitor** component within the **ltm** module using the syntax shown in the following sections.

Create/Modify

```
modify default-node-monitor
    rule [rule syntax]
edit default-node-monitor
  all-properties
```

Display

```
list default-node-monitor
show running-config default-node-monitor
  one-line
  all-properties
```

Description

You can use the **default-node-monitor** component to modify the default monitor that the system applies to any node address to which a monitor is not explicitly assigned.

Examples

modify default-node-monitor rule icmp

Modifies the global default node monitor to use the rule ICMP.

list default-node-monitor

Displays the properties of the global default node monitor.

Options

- **rule**
  Specifies the rule that the system applies to any node that has not been assigned a monitor rule. The default value is **none**.
  You can specify:
  - A single monitor, for example, **modify default-node-monitor rule icmp**.

- Multiple monitors, for example, **modify default-node-monitor rule icmp and tcp_echo**.
- A minimum number of monitors, for example, **modify default-node-monitor rule min 1 of { icmp and tcp_echo }**.

See Also

list, *node*, *modify*, *show*, *tmsh*

eviction-policy

Configures eviction policies to determine when and how to terminate connections.

Syntax

Configure the **eviction-policy** component within the **ltm** module using the syntax shown in the following sections.

Create/Modify

```
create eviction-policy [name]
modify eviction-policy [name]
    app-service [[string] | none]
    low-water [integer]
    high-water [integer]
    slow-flow {
      enabled [true | false]
      eviction-type [count | percent]
      grace-period [integer]
      maximum [integer]
      threshold-bps [integer]
      throttling [enabled | disabled]
    }
    strategies {
      bias-bytes {
        delay [integer]
        enabled [true | false]
      }
      bias-idle {
        enabled [true | false]
      }
      bias-oldest {
        enabled [true | false]
      }
      low-priority-geographies {
        countries [add | delete | modify | replace-all-with] {
          [country-code] ...
        }
        enabled [true | false]
      }
      low-priority-port {
        enabled [true | false]
        ports [add | delete | modify | replace-all-with] {
          [ [name] ] {
            app-service [[string] | none]
            port-number [name | integer]
            protocol [any | sctp | tcp | udp]
          } ...
        }
      }
      low-priority-route-domain {
         enabled [true | false]
         names [add | delete | modify | replace-all-with] {
           [ [route domain name] ] ...
         }
```

```
    }
    low-priority-virtual-server {
       enabled [true | false]
       names [add | delete | modify | replace-all-with] {
         [ [virtual server name] ] ...
       }
    }
  }
```

Display

```
list eviction-policy
list eviction-policy [ [ [name] | [glob] | [regex] ] ...]
    all-properties
    partition
show eviction-policy
show eviction-policy [ [ [name] | [glob] | [regex] ] ...]
    all-properties
    default
```

Delete

```
delete eviction-policy [name]
```

Description

You use the **eviction policy** to specify which flows to terminate when the connection limits for the box are approached. The eviction policy contains strategies which select the flows to terminate. Additionally, the eviction policy defines parameters used to determine when flows are considered to be slow. Slow flows are terminated according to the policy, even when the Big-IP is not under duress and the connection limits are not approached.

When applied to the global context, the **eviction policy** low-water and high-water limits are with respect to memory available on the Big-IP. When applied to a virtual server or a route domain, the limits are with respect to the connection limit on the virtual server or route domain, respectively.

It is possible to monitor slow flows, accumulating metrics on the number of flows under the designated slow flow transfer limit. To do so, enable slow-flows, but disable throttling on the slow flow.

◆ Note

Monitoring or killing slow flows will incur a performance penalty.

◆ Note

The strategies applied here work on a cyclic sweep of all connections on the Big-IP. These do not run at the granularity to guarantee eviction of a particular flow or type of flow, but are statistical and opportunistic.

The **bias-bytes** algorithm attempts to select the flows that have sent and received the fewest bytes on the connection.

The **bias-idle** algorithm attempts to select the flows that have been idle the longest.

The **bias-oldest** algorithm attempts to select the oldest flows.

The **low-priority-geographies** algorithm selects flows that are in low-priority geographies according to the **GeoIP** database loaded onto the box.

The **low-priority-port** algorithm selects flows that are in the provided list of low-priority ports and protocols.

The **low-priority-route-domain** algorithm selects flows that are in the provided list of low-priority route domains.

The **low-priority-virtual-server** algorithm selects flows that are in the provided list of low-priority virtual servers.

Examples

create eviction-policy my_eviction_policy { low-water 70 high-water 80 slow-flow { enabled true threshold-bps 50 throttling disabled } strategies { bias-idle { enabled true } } }

Creates an eviction policy named **my_eviction_policy**, which accumulates statistics on the current number of slow flows but does not terminate any flows that are considered slow. The **bias-idle** algorithm is used to kill flows when the limits on the context are approached. The aggressive sweeper will activate at 80 percent of capacity, and deactivate when load is reduced to 70 percent of capacity.

modify eviction-policy my_eviction_policy { strategies { low-priority-geographies { enabled true countries replace-all-with { AZ BZ } } } }

Modifies the eviction policy named **my_eviction_policy**, enabling the low-priority geography strategy and dropping flows from Azerbaijan (AZ) and Belize (BZ).

delete eviction-policy my_eviction_policy

Deletes the eviction policy named **my_eviction_policy**.

Options

- **app-service**
  Specifies the name of the application service to which the object belongs. The default value is **none**. **Note:** If the **strict-updates** option is **enabled** on the application service that owns the object, you cannot modify or delete the object. Only the application service can modify or delete the object.
- **low-water**
  Specifies the aggressive sweeper activativation threshold as a percentage of total capacity. The allowable range is **50 - 100**, and the low-water

value must be lower than or equal to the **high-water** value. To disable killing flows when limits are met or exceeded, set the low-water and high-water to 100 percent. Default value is 85 percent.

- **high-water**
  Specifies the target maximum load on the context. The adaptive reaper will be more aggressive as this limit is approached. The allowable range is **50 - 100**, and the high-water value must be higher than or equal to the **low-water** value. To disable killing flows when limits are met or exceeded, set the low-water and high-water to 100 percent. Defaults to 95 percent.
- **slow-flow**
  Specifies whether to monitor and possibly remove flows considered to be slow.
  - **enabled**
    If true, the slow-flow monitoring and possible removal are activated. If false, the remaining slow-flow attributes are unused. The default value is **false**.
  - **eviction-type**
    Indicates whether the threshold is based on an absolute count of slow flows, or a percentage of the total flows on the context where the eviction policy is applied. There is no default value.
  - **grace-period**
    Specifies the minimum age of a slow flow before the flow is killed.
  - **maximum**
    Provides the count or percentage at which slow flows will be killed. If **eviction-type** is **count**, this value is the absolute number of slow flows allowed; if **eviction-type** is **percent**, this is the percentage of flows on the context that are allowed to fall under the **threshold-bps** before being killed.
  - **threshold-bps**
    Provides the threshold under which flows are considered to be slow, in bytes per second.
  - **throttling**
    Indicates whether to kill flows that are considered slow. If set to **enabled**, flows that fall under the **threshold-bps** are subject to being killed according to the defined **maximum** number of flows.
- **strategies**
  Defines the strategies to be used to select flows for eviction in the eviction policy.
  - **bias-bytes**
    Defines how to use the bias-bytes eviction strategy.
    - **delay**
      The delay allowed for new flows to transfer content, to prevent killing infant flows.
    - **enabled**
      Specifies whether to use the **bias-bytes** algorithm. If false, the bias-bytes algorithm is not used. The default value is **false**.

- **bias-idle**
  Defines how to use the bias-idle eviction strategy.
  - **enabled**
    Specifies whether to use the **bias-idle** algorithm. If false, the bias-idle algorithm is not used. The default value is **false**.
- **bias-oldest**
  Defines how to use the bias-oldest eviction strategy.
  - **enabled**
    Specifies whether to use the **bias-oldest** algorithm. If false, the bias-oldest algorithm is not used. The default value is **false**.
- **low-priority-geographies**
  Defines how to use the low-priority geographies eviction strategy.
  - **countries**
    Provides a list of country codes considered low-priority candidates to evict, based on GeoIP information.
  - **enabled**
    Specifies whether to use the **low-priority-geographies** algorithm. If false, the low-priority-geographies algorithm is not used. The default value is **false**.
- **low-priority-port**
  Defines how to use the low-priority-port eviction strategy.
  - **enabled**
    Specifies whether to use the **low-priority-port** algorithm. If false, the low-priority-port algorithm is not used. The default value is **false**.
  - **ports**
    Provides a list of ports considered low-priority candidates to evict.
  - **app-service**
    Specifies the name of the application service to which the object belongs. The default value is **none**. **Note:** If the **strict-updates** option is **enabled** on the application service that owns the object, you cannot modify or delete the object. Only the application service can modify or delete the object.
  - **port-number**
    Specifies the port number considered low-priority. The number provided can be either a number (e.g., 80) or a name (e.g., http).
  - **protocol**
    Specifies the protocol considered low-priority. The default value is **any**.
- **low-priority-route-domain**
  Defines how to use the low-priority-route-domain eviction strategy.
  - **enabled**
    Specifies whether to use the **low-priority-route-domain** algorithm. If false, the low-priority-route-domain algorithm is not used. The default value is **false**.

- **names**
  Specifies a list of route domain names considered to be low-priority candidates to evict.

- **low-priority-virtual-server**
  Defines how to use the low-priority-virtual-server eviction strategy.
  - **enabled**
    Specifies whether to use the **low-priority-virtual-server** algorithm. If false, the low-priority-virtual-server algorithm is not used. The default value is **false**.
  - **names**
    Specifies a list of virtual server names considered to be low-priority candidates to evict.

See Also

create, *delete*, *edit*, *list*, *modify*, *show*, *tmsh*, regex, *geoip*

ifile

Configures an iFile.

Syntax

Configure the **iFile** component within the **ltm** module using the syntax shown in the following sections.

Create/Modify

```
create ifile [name]
modify ifile [name]
options:
  app-service [[string] | none]
  description [string]
  file-name [ifile file object name]
edit ifile [ [name] | [glob] | [regex] ] ... ]
    all-properties
    non-default-properties
    one-line
```

Display

```
list ifile
list ifile [ [ [name] | [glob] | [regex] ] ... ]
show running-config ifile
show running-config ifile [ [ [name] | [glob] | [regex] ] ... ]
  all-properties
  non-default-properties
  one-line
```

Delete

```
delete ifile [name]
```

Description

You can use the **ifile** component to configure an iFile. The iFile can then be referenced from an iRule, to allow loading an external file into an iRule.

Examples

create ifile my_ifile file-name ifile_file_object_name

Creates an iFile named **my_ifile**, that gets its contents from the file object **ifile_file_object_name**.

list ifile all-properties

Displays all of the properties of all of the iFiles.

delete ifile my_ifile

Deletes the iFile named **my_ifile**.

Options

- **app-service**
  Specifies the name of the application service to which the iFile belongs. The default value is **none**. **Note:** If the **strict-updates** option is **enabled** on the application service that owns the object, you cannot modify or delete the iFile. Only the application service can modify or delete the iFile.
- **description**
  User defined description.
- **file-name**
  The name of the iFile File Object that this iFile uses.

See Also

create, *delete*, *edit*, glob, *list*, *modify*, regex, *tmsh*

lsn-log-profile

Configures a Large-Scale Network Address Translation logging profile.

Syntax

Create/Modify

```
create lsn-log-profile [name]
modify lsn-log-profile [name | all]
    app-service [[string] | none]
    start-outbound-session {
        action [disabled | enabled | backup-allocation-only]
        elements [add | delete | replace-all-with] {
            destination
        }
    }
    end-outbound-session {
        action [disabled | enabled | backup-allocation-only]
        elements [add | delete | replace-all-with] {
            destination
        }
    }
    start-inbound-session {
        action [disabled | enabled | backup-allocation-only]
    }
    end-inbound-session {
        action [disabled | enabled | backup-allocation-only]
    }
    quota-exceeded {
        action [disabled | enabled ]
    }
    errors {
        action [disabled | enabled ]
    }
edit lsn-log-profile [ [ [name] | [glob] | [regex] ] ... ]
    all-properties
    non-default-properties
reset-stats lsn-log-profile
reset-stats lsn-log-profile [ [ [name] | [glob] | [regex] ] ... ]
```

Display

```
list lsn-log-profile
list lsn-log-profile [ [ [name] | [glob] | [regex] ] ... ]
show running-config lsn-log-profile
show running-config lsn-log-profile [ [ [name] | [glob] | [regex] ] ... ]
    all-properties
    non-default-properties
    one-line
```

Delete

```
delete lsn-log-profile [name | all]
```

Description

A LSN log profile allows fine grain control of the logging for LSN translation events. When attached to an LSN pool, you can control the events to enable logging, and the elements in the log entry.

Examples

create ltm lsn-log-profile my_lsn_log_profile end-inbound-session { action enabled } end-outbound-session { action enabled }

Creates the LSN log profile **my_lsn_log_profile** that generates log entries for both inbound and session when the translation session ends.

delete lsn-log-profile my_lsn_log_profile

Deletes the LSN log profile named **my_lsn_log_profile**.

Options

- **app-service**
  Specifies the name of the application service to which this object belongs. The default value is **none**.

◆ Note

*If the **strict-updates** option is **enabled** on the application service that owns the object, you cannot modify or delete this object. Only the application service can modify or delete this object.*

- **events**
  The type of LSN translation events available for logging control.
  - **start-outbound-session**
    Event for start of outbound translation session, when the outbound flow is created.
  - **end-outbound-session**
    Event for end of outbound translation session, when the outbound flow is deleted.
  - **start-inbound-session**
    Event for start of incoming connection to a translated address.
  - **end-inbound-session**
    Event for end of incoming connection to a translated address.
  - **quota-exceeded**
    Event for when client exceeded allocated resource limit.
  - **errors**
    Event for when LSN encountered errors while attempting translation for clients.

- **action**
  Specify the logging action to be taken when a particular event is encountered.
  - **enabled**
    Logging is enable for the event, whether translation is from the primary pool member or backup pool member.
  - **backup-allocation-only**
    Logging is enable for the event, when translation is take from backup pool member only.
  - **disabled**
    Logging is disable for the event.
- **elements**
  Optional elements that can be added to the log message.
- **regex**
  Displays the items that match the regular expression. The regular expression must be preceded by an at sign (@[regular expression]) to indicate that the identifier is a regular expression. See **help regex** for a description of regular expression syntax.

See Also

lsn-pool, *create*, *delete*, *edit*, glob, *list*, *ltm*, *modify*, regex, *show*, *tmsh*

lsn-pool

Configures a Large-Scale Network Address Translation (or Carrier-Grade Network Address Translation) pool.

Syntax

Create/Modify

```
create lsn-pool [name]
modify lsn-pool [name | all]
    app-service [[string] | none]
    backup-members
      [add | delete | replace-all-with] {
        [ip address/prefix length] ...
    }
    client-connection-limit [integer value]
    description [string]
    egress-interfaces
      [add | delete | replace-all-with] {
        [interface name] ...
    }
    egress-interfaces-disabled
    egress-interfaces-enabled
    hairpin-mode [enabled | disabled]
    icmp-echo [enabled | disabled]
    inbound-connections [automatic | explicit | disabled]
    log-publisher [log publisher name | none]
    log-profile [log profile name | none]
    members
      [add | delete | replace-all-with] {
        [ip address/prefix length] ...
    }
    mode [deterministic | napt | pba]
    persistence {
      mode [none | address | address-port]
      timeout [integer]
    }
    pcp {
      profile [ name | none ]
      selfip [ name | none]
      dslite_tunnel [ name | none ]
    }
    port-block-allocation  {
       block-idle-timeout [integer]
       block-lifetime [integer]
       block-size [integer]
       client-block-limit [integer]
       zombie-timeout [integer]
    }
    route-advertisement [enabled | disabled]
    translation-port-range [integer low:integer high | integer]
edit lsn-pool [ [ [name] | [glob] | [regex] ] ... ]
    all-properties
    non-default-properties
```

```
reset-stats lsn-pool
reset-stats lsn-pool [ [ [name] | [glob] | [regex] ] ... ]
```

Display

```
list lsn-pool
list lsn-pool [ [ [name] | [glob] | [regex] ] ... ]
show running-config lsn-pool
show running-config lsn-pool [ [ [name] | [glob] | [regex] ] ... ]
    all-properties
    non-default-properties
    one-line
show lsn-pool
show lsn-pool [ [ [name] | [glob] | [regex] ] ... ]
    (default | exa | gig | kil | meg | peta | raw | tera | yotta | zetta)
    detail
    field-fmt
```

Delete

```
delete lsn-pool [name | all]
```

Description

A large-scale NAT (LSN) pool is a set of networks and port numbers that the BIG-IP system uses as public-side addresses and ports. When you assign an LSN pool to a virtual server, the virtual server's clients have their private addresses (and/or ports) translated to a public address and/or port from the LSN pool. The public-side addresses and ports in the LSN pool are called *translation addresses and ports*.

Examples

create lsn-pool my_lsn_pool1 mode napt persistence { mode address-port timeout 600 } members add { 10.10.10.0/24 10.10.20.0/24 } translation-port-range 4000:5000 client-connection-limit 100

Creates the LSN pool **my_lsn_pool1** that contains the translation addresses in the range of (members) **10.10.10.0/24** and **10.10.20.0/24**, translation port range **4000-5000**, with a client connection limit of **100** connections per client. The translated address and port are persisted for 600 seconds. This LSN pool operates in **NAPT** mode (Network Address and Port Translation mode), which is the default mode if not specified.

delete lsn-pool my_lsn_pool1

Deletes the LSN pool named **my_lsn_pool1**.

Options

- **app-service**
  Specifies the name of the application service to which this object belongs. The default value is **none**.

◆ Note

*If the **strict-updates** option is **enabled** on the application service that owns the object, you cannot modify or delete this object. Only the application service can modify or delete this object.*

- **backup-members**
  Specifies translation IP addresses available in the backup pool which is used by DNAT translation mode if DNAT mode translation fails and falls back to NAPT mode. This is a collection of IP prefixes with their prefix lengths.
- **client-connection-limit**
  The maximum number of simultaneous translated connections a client or subscriber is allowed to have.
- **description**
  User defined description.
- **egress-interfaces**
  The set of interfaces on which the source address translation is allowed or disallowed. If egress-interfaces-enabled is specified, the source address translation is allowed only on the specified set of interfaces. If egress-interfaces-disabled is specified, source address translation is disabled on specified interfaces.
- **egress-interfaces-disabled**
  Source address translation is not allowed on the interfaces specified in the egress-interfaces set.
- **egress-interfaces-enabled**
  Source address translation is allowed on the interfaces specified in the egress-interfaces set.
- **glob**
  Displays the items that match the **glob** expression. See **help glob** for a description of **glob** expression syntax.
- **hairpin-mode**
  Enable or disable hairpinning for incoming connections.
  When a client sends a packet to another client in the same private network, hairpin mode sends the packet directly to the destination client's private address; the BIG-IP system immediately translates the packet's public-side destination address. Rather than going out to the public network and coming back later for translation, the packet takes a hairpin turn at the BIG-IP device.
- **icmp-echo**
  Enable or disable ICMP echo on translated addresses.

- **inbound-connections**
  Modifies the inbound-connection mode for incoming connections to translation endpoints. A *translation endpoint* is the public-side address and port (X':x') for a private-side address (X:x). You can allow one of three algorithms for managing inbound connections:
  - **Automatic**
    creates inbound mappings automatically from outbound traffic and allows inbound connections. Consider an outbound mapping from X:x to X':x'. If a connection comes from X:x through X':x', the BIG-IP system automatically creates a reverse mapping from X':x' back to X:x. A public-side station can respond through the X':x' address. This allows the BIG-IP system to provide Endpoint Independent Filtering (EIF) as defined in section 5 of RFC 4787 (http://tools.ietf.org/html/rfc4787#section-5).
  - **Explicit**
    only allows inbound connections for mappings that are explicitly created by another party, such as iRules or a PCP request. For example, if a PCP request creates a mapping of X:x to X':x' and the client at X:x uses it, an external caller can respond to the client through X':x'. However, if a client at M:m automatically makes a NAT'ed connection through M':m', the BIG-IP does not support an inbound connection from M':m' back to M:m.
  - **Disabled**
    disables inbound connections to translation end-points (X':x'). If there is a mapping of X (a private-side IP address) to X' (a public-side IP), connections can only go out from X through X'. If a public-side recipient tries to answer at the client's public-side X' address, the BIG-IP system does not map X' back to X. The inbound connection never happens.
    Port Control Protocol (PCP) is not supported if you use this setting.
- **log-publisher**
  Specify the name of the log publisher which logs translation events. See **help sys log-config** for more details on the logging sub-system. Use the *publisher* component to set up a log publisher.
- **log-profile**
  Specify the name of the LSN log profile which controls the logging of translation events. See **help ltm lsn-log-profile** for more details on the logging profile sub-system. Use the ltm lsn-log-profile profile component to set up a LSN log profile.
- **members**
  Specifies the set of translation IP addresses available in the pool. This is a collection of IP prefixes with their prefix lengths. All public-side addresses come from the subnets you enter in this property.
- **mode**
  Specifies which kind of translation address mapping is performed when an address is translated. Available options are NAPT, Deterministic, and PBA.

- **NAPT**
  (Network Address Port Translation) assigns translation addresses and ports in round-robin fashion. The algorithm first cycles through translation addresses and then through translation ports.
- **Deterministic**
  (DNAT) is a reversible translation method. A given client address and port always translates to a particular public address and port from the LSN pool. This method has the following restrictions:
  - it is only available for NAT44 translations,
  - it does not support connections through DS-Lite tunnels,
  - subscriber connections must be received over a VLAN with the property, **cmp-hash**, set to "source ip,"
  - the egress to the Internet must be over a VLAN with the property, **cmp-hash**, set to "dest ip,"
  - any virtual server (*virtual*) that uses this LSN pool must have a **source** property set to an IP prefix containing fewer than 231 addresses. For example, the source cannot be 0.0.0.0/0.
- **PBA**
  (Port Block Allocation) assigns ‘blocks’ of the translation addresses and ports to individual clients. All client connections are restricted to the allocated port blocks. Only block allocations and deallocations are logged in order to reduce the volume of logs.
  - subscriber connections must be received over a VLAN with the property, **cmp-hash**, set to "source ip,"
  - the egress to the Internet must be over a VLAN with the property, **cmp-hash**, set to "dest ip,"

You can access your VLAN configurations through the *vlan* component. You can find the VLANs used by your virtual server by showing or listing the *virtual* component.

- **name**
  Specifies a unique name for the lsn-pool component. This option is required for the commands **create**, **delete**, and **modify**.
- **persistence**
  Configure the persistence settings for LSN translation entries. Persistence is the preservation of a public-side IP address for a client from session to session.
- **persistence.mode**
  Configure the persistence mode for LSN translation entries. You can enter **address**, **address-port**, or **none**.

- **address**
  causes the BIG IP software to attempt to keep the IP address persistent but not necessarily the port. If a client's private IP address:port combination is X:x, it's public-side address may be X':a in one session, X':b in the next session, X':c in a third session, and so on.
- **address-port**
  causes the BIG IP software to attempt to keep the IP address and port persistent. If a client's private IP address:port combination is X:x, and it's public-side address is X':x' in the first session, it remains X':x' in all future sessions.
  This is called "Endpoint Independent Mapping" in RFC 4787 (http://www.ietf.org/rfc/rfc4787.txt).
  This is the only supported setting for PCP, which you configure with the **pcp** property.
- **none**
  prevents the BIG IP software from attempting any IP address or port persistence. An address:port combination of X:x is never guaranteed to have the same public-side address or port in two sessions.

◆ **persistence.timeout**
After the most-recent session where address:port X:x translated to X':x' on the public side, a timer begins. If the timer expires before X:x has another session, X' or x' may be used as the public side of another address:port. Use this parameter to set the timeout (in seconds) for address and port persistence.

◆ **pcp**
A Port Control Protocol (PCP) client can set (or at least learn) its own translation (public-side) IP address and/or port. It can also set the address and/or port of a third-party client. PCP is defined in RFC 6887 (see http://www.ietf.org/rfc/rfc6887.txt).

◆ **pcp.profile**
Specifies the PCP profile to use for this LSN pool. This PCP profile defines the settings to use for communication with PCP clients. Use the **create ltm profile pcp** command to create a new PCP profile.
PCP requires a profile (defined with this property) and either a **pcp.selfip** or a **pcp.dslite** tunnel where clients can send their PCP requests.
If you remove this profile option, you must specifically remove any **pcp.selfip** or **pcp.dslite** tunnel, too.

◆ **pcp.selfip**
Specifies the PCP Server self-IP address for this LSN pool. The virtual server's clients send their PCP packets to this address. Use the **create net self** command to create a self-IP address, then use that address for this parameter. Choose a self-IP address in a VLAN that is reachable by the virtual server's clients.

◆ **pcp.dslite**
Specifies a DS-LITE tunnel for PCP packets. Whenever a client sends a PCP packet through this tunnel, the BIG-IP device uses the PCP profile you choose with the **pcp.profile** property.
A DS-LITE tunnel places each IPv4 packet into the payload of an IPv6

packet. The IPv6 packet carries the IPv4 packet between customer equipment and the BIG-IP system, which then removes the IPv4 packet, uses NAT to translate its IPv4 addresses, and sends it to its destination. You cannot use this property if the **mode** property is set to **Deterministic**.

- **port-block-allocation**
  Configures the port block settings for PBA mode.
- **port-block-allocation.block-idle-timeout**
  Configures the time after the last connection using the block is freed that the block assignment expires. The default value is 3600 seconds.
- **port-block-allocation.block-lifetime**
  Configures the timeout after which the block is no longer used for new port allocations. The block becomes a zombie block. The default is 0 which corresponds to an infinite timeout.
- **port-block-allocation.block-size**
  Configures the number of ports in a block. The default value is 64.
- **port-block-allocation.client-block-limit**
  Configures the number of blocks that can be assigned to a single subscriber IP address. The default value is 1.
- **port-block-allocation.zombie-timeout**
  Configures the timeout after which connections using the zombie block are killed. After connections are killed zombie block is freed after port-block-allocation.block-idle-timeout. This parameter is unused unless the port-block-allocation.block-lifetime is set. The default value is 0 which corresponds to infinite timeout.
- **regex**
  Displays the items that match the regular expression. The regular expression must be preceded by an at sign (@[regular expression]) to indicate that the identifier is a regular expression. See **help regex** for a description of regular expression syntax.
- **route-advertisement**
  Specifies whether route advertisement is enabled or disabled for translated IP addresses.
- **translation-port-range**
  Specifies the range of port numbers available for use with translation IP addresses.

See Also

pcp, *virtual*, *self*, *vlan*, *create*, *delete*, *edit*, glob, *list*, *ltm*, *modify*, regex, *reset-stats*, *show*, *tmsh*

nat

Configures network address translation (NAT) for the Local Traffic Manager.

Syntax

Configure the **nat** component within the **ltm** module using the syntax in the following sections.

Create/Modify

```
create nat [name]
modify nat [name]
    app-service [[string] | none]
    arp
    auto-lasthop [default | enabled | disabled ]
    description [string]
    [enabled | disabled]
    originating-address [ip address]
    translation-address [ip address]
    traffic-group [[string] | default | non-default | none]
    vlans [enabled | disabled]
    vlans-disabled
    vlans-enabled
reset-stats nat
reset-stats nat [ [ [name] | [glob] | [regex] ] ... ]
edit nat [ [ [name] | [glob] | [regex] ] ... ]
    all-properties
    non-default-properties
```

Display

```
list nat
list nat [ [ [name] | [glob] | [regex] ] ... ]
show running-config nat
show running-config nat [ [ [name] | [glob] |
                            [regex] ] ... ]
    all-properties
    non-default-properties
    one-line
    partition
show nat
show nat [name]
    (default | exa | gig | kil | meg | peta | raw | tera | yotta | zetta)
    field-fmt
```

Delete

```
delete nat [name]
```

Description

A network address translation (NAT) defines a mapping between an originating IP address and an IP address that you specify.

A primary reason for defining a NAT is to allow one of the servers in the server array behind the traffic management system to start communication with a computer in front of, or external to, the system.

Examples

create nat new_nat translation-address 10.0.140.100 originating-address 11.0.0.100

The node behind the system with the IP address **10.0.140.100** has a presence in front of the BIG-IP® System as IP address **11.0.0.100**.

delete nat new_nat

Permanently deletes the NAT from the system configuration.

Additional Restrictions

The **nat** component has the following additional restrictions:

- A virtual server cannot use the IP address specified in the NAT.
- A NAT should not use an IP address of a BIG-IP system.
- A NAT cannot use an originating or translated IP address defined for and used by a SNAT or another NAT.
- You must delete a NAT before you can redefine it.

Options

- **app-service**
  Specifies the name of the application service to which the NAT belongs. The default value is **none**. **Note:** If the **strict-updates** option is **enabled** on the application service that owns the object, you cannot modify or delete the NAT. Only the application service can modify or delete the NAT.
- **arp**
  Enables or disables Address Resolution Protocol (ARP).
- **description**
  User defined description.
- **[enabled | disabled]**
  Enables or disables the NAT. The default value is **enabled**.

- **glob**
  Displays the items that match the **glob** expression. See **help glob** for a description of **glob** expression syntax.
- **inherited-traffic-group**
  Indicates if the **traffic-group** is inherited from the parent folder. This property is read only.
- **originating-address**
  Specifies the IP address from which traffic is being initiated.
- **regex**
  Displays the items that match the regular expression. The regular expression must be preceded by an at sign (@[regular expression]) to indicate that the identifier is a regular expression. See **help regex** for a description of regular expression syntax.
- **traffic-group**
  Specifies the traffic group of the failover device group on which the NAT is active. The default traffic group is inherited from the containing folder.
- **translation-address**
  Specifies the IP address that is translated or mapped, and the IP address to which it is translated or mapped. This option is required when creating a NAT. This option may not be changed after the **nat** has been created.
- **unit**
  Specifies the unit in a redundant system. Derived from **traffic-group**. This property is read only.
- **vlans**
  Specifies a list of existing VLANs on which access to the NAT is enabled or disabled. A NAT is accessible on all VLANs by default.
- **vlans-disabled**
  Indicates the NAT is disabled on the list of VLANs.
- **vlans-enabled**
  Indicates the NAT is enabled on the list of VLANs.

See Also

create, *delete*, *edit*, glob, *list*, *snat*, *snat-translation*, *modify*, regex, *reset-stats*, *show*, *tmsh*

node

Configures node addresses and services.

Syntax

Configure the **node** component within the **ltm** module using the syntax in the following sections.

Create/Modify

```
create node [name]
modify node [name]
     address [ip address]
     app-service [[string] | none]
     connection-limit [integer]
     description [string]
     [down | up]
     dynamic-ratio [integer]
     fqdn {
         name [string]
         address-family [ipv4 | ipv6]
         autopopulate [enabled | disabled]
         down-interval [integer]
         interval [integer]
     }
     logging [enabled | disabled]
     monitor [ [name] | none]
     rate-limit [integer]
     ratio [integer]
     session [user-enabled | user-disabled]
     state [user-down | user-up]
     metadata
       [add | delete | modify] {
         [metadata_name ... ] {
           value [ "value content" ]
           persist [ true | false ]
         }
     }
reset-stats node
reset-stats node [ [ [ip address] | [glob] | [regex] ] ... ]
edit node [ [ [name] | [glob] | [regex] ] ... ]
    all-properties
    non-default-properties
mv node [ [[source-name] [destination-name]] | [[name] to-folder [folder-name]] |
[[name...name] to-folder [folder-name]] ]
    to-folder
```

Display

```
list node
list node [ [ [name] | [glob] | [regex] ] ... ]
show running-config node
show running-config node [ [ [name] | [glob] | [regex] ] ... ]
    all-properties
```

```
    non-default-properties
    one-line
    partition
show node
show node [name]
    all-properties
    (default | exa | gig | kil | meg | peta | raw | tera | yotta | zetta)
    field-fmt
```

Delete

```
delete node [name]
```

Description

Displays information about nodes, and sets attributes of nodes and node IP addresses.

Examples

list node all-properties

Displays all of the properties of all of the nodes.

modify node all monitor none

Removes all monitor associations from nodes.

create node myNode address 10.10.10.15

Creates a node named myNode with an IP address of 10.10.10.15.

modify node myNode monitor none

Removes all monitor associations from the node, myNode.

show node

Displays statistics and status for all nodes in the system configuration.

show node all-properties

Displays statistics and status for all nodes in the system configuration. If the system includes Packet Velocity® ASIC (PVA) and PVA Assist capabilities, this command displays status and statistics for that feature.

mv /ltm node /Common/10.10.10.15 to-folder /Common/all_nodes

Moves the node **10.10.10.15** to a folder named **all_nodes**, where **all_nodes** has already been created under **/Common**.

◆ Note

If you wish to change the name of the node, you must use the nodes same IP Address or a name that does not represent an IP Address that does not match the address configured on the node.

Please refer to the **mv** manual page for additional examples on how to use the mv command.

Options

- **address**
  Specifies the IP address of the node.
- **app-service**
  Specifies the name of the application service to which the node belongs. The default value is **none**. **Note:** If the **strict-updates** option is **enabled** on the application service that owns the object, you cannot modify or delete the node. Only the application service can modify or delete the node.
- **connection-limit**
  Specifies the maximum number of connections that a node or node address can handle. The default value is **0** (zero).
- **description**
  Specifies a user-defined description.
- **[down | up]**
  Marks the node **up** or **down**. The default value is **down**.
- **dynamic ratio**
  Sets the dynamic ratio number for the node. The ratio weights are based on continuous monitoring of the servers and are therefore continually changing. The default value is **1**.
  Dynamic Ratio load balancing can currently be implemented on RealNetworks RealServer platforms, on Windows platforms equipped with Windows Management Instrumentation (WMI), or on a server equipped with either the UC Davis SNMP agent or Windows 2000 Server SNMP agent.
- **glob**
  Displays the items that match the **glob** expression. See **help glob** for a description of **glob** expression syntax.
- **metadata**
  Associates user defined data, each of which has a name and value pair and persistence. The default value is **persistent**, which saves the data to the config file.
- **fqdn**
  Specifies the attributes for defining a fully qualified domain name for the node.
  - **name**
    Specifies the fully-qualified domain name of the node.
  - **address-family**
    Specifies whether the fqdn should consider IPv4, IPv6, or IP-agnostic address family.
  - **autopopulate**
    Specifies whether a node defined by a fully-qualified domain name should automatically scale to the set of IP addresses returned by the DNS query. If **disabled**, only one ephemeral node is generated from the first IP address returned by DNS. The default is **disabled**.

- **interval**
  Specifies the interval to instantiate DNS queries on a fully-qualified domain name. The default is the TTL.
- **down-interval**
  Specifies the interval for the domain name resolution operation when a DNS query fails.

- **logging**
  Specifies whether the monitor applied should log its actions. Logs are stored in /var/log/monitors/ and are regularily rotated and compressed. The default value is **disabled**. This option isn't a part of configuration and will reset to **disabled** on load. This option doesn't sync.
- **monitor**
  Specifies the name of the monitor that you want to associate with the node. The default value is **none**.
- **partition**
  Displays the administrative partition in which the node object resides.
- **rate-limit**
  Specifies the maximum number of connections per second allowed for a node or node address. The default value is 'disabled'.
- **ratio**
  Specifies the fixed ratio value used for a node during Ratio load balancing. The default value is **1**.
- **regex**
  Displays the items that match the regular expression. The regular expression must be preceded by an at sign (@[regular expression]) to indicate that the identifier is a regular expression. See **help regex** for a description of regular expression syntax.
- **session**
  Establishing a session with a node is establishing the ability of the client to persist to the node when making new connections. When a node is session disabled, clients that have already established sessions with the node may create new connections, but a client that has not already established a session may not create a new one (or make a connection which would create a new session). This feature is used to gently drain connections from a node, typically as part of a maintenance operation. The default value is **user-enabled**.
- **state**
  Specifies the current state of the node. Use **user-down** to indicate that the node may not handle any new connections. Use **user-up**, after using **user-down**, to indicate that the node may accept new connections.
- **to-folder**
  This is used with the **mv** command to specify a **folder** in which to move the **node** to.

◆ Note

nodes *can be moved to any folder under* ***/Common****, but dependencies upon it may restrict moving it out of* ***/Common****.*

See Also

create, *delete*, *edit*, glob, *list*, *pool*, *modify*, *mv*, regex, *reset-stats*, *show*, *tmsh*

policy

Configures a policy for Centralized Policy Manager.

Syntax

Modify the policy component within the **ltm** module using the syntax shown in the following sections.

For additional details, refer to Local Traffic Policy documentation on the AskF5 knowledge base at http://support.f5.com.

Create/Modify

```
create policy [name]
modify policy [name]
  controls [add | delete | modify | replace-all-with] {
            none | forwarding | caching | compression | acceleration | asm |
            avr | l7dos | classification | request-adaptation |
            response-adaptation | server-ssl
  }
  requires [add | delete | modify | replace-all-with] {
            none | http | tcp | client-ssl
  }
  rules [add | delete | modify | replace-all-with] {
        [ [string] ] {
           ordinal [ integer ] | app-service [ string ] |
           conditions [add | delete | modify | replace-all-with] {
            [ integer ] {
            app-service | request | response | all | name | value | header |
            scheme | host | port | path | query-string | extension |
            path-segment | query-parameter | unnamed-query-parameter | major |
            minor | code | text | domain | expiry | version | username |
            password | protocol | cipher | cipher-bits | rtt | mss | vlan |
            vlan-id | route-domain | geoip | tcp | client-ssl | http-method |
            http-uri | http-version | http-status | http-host | http-header |
            http-referer | http-cookie | http-set-cookie | http-basic-auth |
            case-insensitive | case-sensitive | external | index | internal |
            local | missing | not | present | remote | values | equals |
            starts-with | ends-with | contains | less | greater |
            less-or-equal | greater-or-equal
           } |
           actions [add | delete | modify | replace-all-with] {
            [ integer ] {
            request | response | all | name | value | header | scheme | host |
            port | path | query-string | extension | path-segment |
            query-parameter | unnamed-query-parameter | major | minor | code |
            text | domain | expiry | version | username | password | protocol |
            cipher | cipher-bits | rtt | mss | vlan | vlan-id | route-domain |
            tcp | client-ssl | http-method | http-uri | http-version |
            http-status | http-host | http-header | http-referer | http-cookie |
            http-set-cookie | http-basic-auth
           }
  }
  strategy [[string] | none]
```

Display

```
list policy
list policy [ [ [name] | [glob] | [regex] ] ... ]
  all-properties
  non-default-properties
  one-line
  partition
show policy
show policy [name]
  all-properties
  (default | exa | gig | kil | meg | peta | raw | tera | yotta | zetta)
  detail
  field-fmt
```

Delete

```
delete policy [name]
```

◆ Note

You must remove all references to a policy before you can delete it.

Description

You can use this **policy** component to configure the policy definitions on the Local Traffic Manager. A load balancing policy is a logical set of rules that you group together to process and direct traffic.

Examples

create policy my_policy controls add { request-adaptation } requires add { http } strategy my_strategy

Creates a Local Traffic Manager policy named **my_policy** which controls request-adaptation of connections to a virtual which is required to have an http policy. The strategy determining policy actions is my_strategy.

delete policy my_policy

Deletes the policy named **my_policy**.

show policy

Displays statistics and status for all Local Traffic Manager policies in the system configuration.

show policy all-properties

Displays statistics and status for all Local Traffic Manager policies in the system configuration.

Note that if the system includes Packet Velocity® ASIC (PVA) and PVA Assist capabilities, this command displays status and statistics for that feature.

list policy my_policy

Displays properties of the policy named **my_policy**.

Options

- **app-service**
  Specifies the name of the application service to which the policy belongs. The default value is **none**. **Note:** If the **strict-updates** option is **enabled** on the application service that owns the object, you cannot modify or delete the policy. Only the application service can modify or delete the policy.
- **controls**
  Specifies the set of features the policy controls. Controls settings aid validation and help determine choices for operands, conditions and actions you can use to define the associated rules. Controls settings also help detect/prevent conflicts between multiple policies on the same virtual server.
  - **none**
    No features are controlled by this policy.
  - **forwarding**
    Forwarding is controlled by this policy.
  - **caching**
    Caching is controlled by this policy.
  - **compression**
    Compression is controlled by this policy.
  - **acceleration**
    Acceleration is controlled by this policy.
  - **asm**
    Application Security Management is controlled by this policy.
  - **avr**
    Application Visibility Reporting is controlled by this policy.
  - **l7dos**
    Layer 7 Dos Protection is controlled by this policy.
  - **classification**
    Classification is controlled by this policy.
  - **request-adaptation**
    Request Adaptation is controlled by this policy.
  - **response-adaptation**
    Response Adaptation is controlled by this policy.
  - **server-ssl**
    Server SSL behavior is controlled by this policy.
- **description**
  User defined description.
- **requires**
  Specifies the required profile types. A policy is applicable to certain types of virtual servers. The Requires settings validate that policy can be

applied to a virtual server (for example, the virtual server has the set of required profiles needed to execute this policy). In addition, the Requires settings govern the choices for operands, conditions and actions you can use to define the associated rules.

- **none**
  No profiles need to be attached to a virtual with this policy.
- **http**
  An HTTP profile needs to be attached to a virtual with this policy.
- **tcp**
  A TCP profile needs to be attached to a virtual with this policy.
- **client-ssl**
  A Client-SSL profile needs to be attached to a virtual with this policy.

◆ **rules**
In the case where multiple rules match a strategy, determines which actions get executed, in what order.

- **ordinal**
  The number used to rank the rules according to precedence.
- **conditions**
  The conditions under which the rule applies. Specify the conditions you want to include in the Conditions list. You can also edit and delete existing condition definitions.
- **app-service**
  Specifies the name of the application service to which the condition belongs. The default value is **none**. **Note:** If the **strict-updates** option is **enabled** on the application service that owns the object, you cannot modify or delete the condition. Only the application service can modify or delete the condition.
- **request**
  The condition is matched on a request to the Virtual Server.
- **response**
  The condition is matched on a response to the Virtual Server.
- **geoip**
  Specify a condition based upon properties of the geographical location of the IP address, such as continent code, country code, city, region, or organization. Parameters are available to identify which interface (external[default] or internal) and address (remote[default] or local) to use.
- **all**
  Specifies that all items should be selected.
- **name**
  Specifies that the name should be selected.
- **value**
  Specifies that a value should be selected.
- **header**
  Specifies that a header should be selected.

- **scheme**
  Specifies that a scheme should be selected.
- **host**
  Specifies that a host should be selected.
- **port**
  Specifies that a port should be selected.
- **path**
  Specifies that a path should be selected.
- **query-string**
  Specifies that a query string should be selected.
- **extension**
  Specifies that an extension should be selected.
- **path-segment**
  Specifies that a path segment should be selected.
- **query-parameter**
  Specifies that a query parameter should be selected.
- **unnamed-query-parameter**
  Specifies that an unnamed query parameter should be selected.
- **major**
  Specifies that a major should be selected.
- **minor**
  Specifies that a minor should be selected.
- **code**
  Specifies that code should be selected.
- **text**
  Specifies that text should be selected.
- **domain**
  Specifies that a domain should be selected.
- **expiry**
  Specifies that an expiry should be selected.
- **version**
  Specifies that a version should be selected.
- **username**
  Specifies that a username should be selected.
- **password**
  Specifies that a password should be selected.
- **protocol**
  Specifies that a protocol should be selected.
- **cipher**
  Specifies that a cipher should be selected.
- **cipher-bits**
  Specifies that cipher bits should be selected.
- **rtt**
  Specifies that the round trip time should be selected.

- **mss**
  Specifies that the maximum segment size should be selected.
- **vlan**
  Specifies that the Vlan should be selected.
- **vlan-id**
  Specifies that the Vlan ID should be selected.
- **route-domain**
  Specifies that the route domain should be selected.
- **tcp**
  Specifies that tcp connections should be examined.
- **client-ssl**
  Specifies that tcp connections should be examined.
- **http-method**
  Specifies that HTTP methods should be examined.
- **http-uri**
  Specifies that HTTP URIs should be examined.
- **http-version**
  Specifies that HTTP versions should be examined.
- **http-status**
  Specifies that HTTP statuses should be examined.
- **http-host**
  Specifies that HTTP hosts should be examined.
- **http-header**
  Specifies that HTTP headers should be examined.
- **http-referer**
  Specifies that HTTP referers should be examined.
- **http-cookie**
  Specifies that HTTP cookies should be examined.
- **http-set-cookie**
  Specifies that HTTP set cookies should be examined.
- **http-basic-auth**
  Specifies that HTTP basic authorization should be examined.

◆ **actions**
Indicates the actions specified for the rule.

- **response**
  Specifies that the action should be taken on a response from the Virtual Server in a connection.
- **request**
  Specifies that the action should be taken on a request from the Virtual Server in a connection.
- **insert**
  Specifies that a value should be inserted.
- **replace**
  Specifies that a value should be replaced.

- **apply**
  Specifies that an feature should be applied.
- **add**
  Specifies that a value should be added.
- **classify**
  Specifies that a value should be classified.
- **remove**
  Specifies that a value should be removed.
- **select**
  Specifies that a value should be selected.
- **enable**
  Specifies that a feature should be enabled.
- **disable**
  Specifies that a feature should be disabled.
- **redirect**
  Specifies that a connection should be redirected.
- **write**
  Specifies that a value should be written.
- **reset**
  Specifies that a connection should be reset.
- **event**
  Specifies that an event should occur.
- **set-variable**
  Specifies that an variable should be set.
- **policy**
  Specifies that a policy should be applied.
- **rule**
  Specifies that a rule should be applied.
- **action-id**
  Specifies that an action with a particular id should be applied.
- **name**
  Specifies that a name should be given.
- **index**
  Specifies that an indexed value in a list should be changed.
- **all**
  Specifies that the action should be applied to every value selected.
- **default**
  Specifies that a default action should be taken.
- **next**
  Specifies that the next value should be modified.
- **pin**
  Specifies that a connection should be pinned.
- **value**
  Specifies that a value should be set.

- **path**
  Specifies that a path should be set.
- **extension**
  Specifies that an extension should be used.
- **scheme**
  Specifies that a scheme should be adopted.
- **host**
  Specifies that a host should be set.
- **domain**
  Specifies that a domain should be set.
- **expiry**
  Specifies that an expiry should be set.
- **location**
  Specifies that a location should be set.
- **query-string**
  Specifies that a query string should be set.
- **port**
  Specifies that a port should be set.
- **status**
  Specifies that a status should be set.
- **content**
  Specifies that content should be set.
- **ifile**
  Specifies that an ifile should be run.
- **code**
  Specifies that a code should be set.
- **text**
  Specifies that text should be set.
- **username**
  Specifies that a username should be set.
- **password**
  Specifies that a password should be set.
- **profile**
  Specifies that a profile should be set.
- **from-profile**
  Specifies that a from profile should be set.
- **internal-virtual**
  Specifies that the connection should be sent through an internal virtual server.
- **policy**
  Specifies that a policy should be invoked.
- **script**
  Specifies that a script should be invoked.

- **cookie**
  Specifies that a cookie should be set.
- **expression**
  Specifies that an expression should be set.
- **message**
  Specifies that a message should be set.
- **pool**
  Specifies that the connection should go to a specific pool.
- **clone-pool**
  Specifies that the connection should cloned and simultaneously sent to another pool.
- **node**
  Specifies that a node should be set.
- **member**
  Specifies that a member should be set.
- **snat**
  Specifies that snatting policy should be set.
- **snatpool**
  Specifies that a snat pool should be set.
- **vlan**
  Specifies that a Vlan should be set.
- **vlan-id**
  Specifies that a Vlan ID should be set.
- **virtual**
  Specifies that a Virtual should be set.
- **rateclass**
  Specifies that a rateclass should be applied.
- **nexthop**
  Specifies that a nexthop should be set.
- **query-parameter**
  Specifies that a query parameter should be set.
- **unnamed-query-parameter**
  Specifies that an unnamed query parameter should be set.
- **version**
  Specifies that a version should be set.
- **application**
  Specifies that an application should be set.
- **category**
  Specifies that a category should be set.
- **protocol**
  Specifies that a protocol should be set.
- **defer**
  Specifies that a connection should be deferred.

- **local**
  Specifies that a local action should be taken.
- **internal**
  Specifies that an internal action should be taken.
- **http**
  Specifies that HTTP connections should be modified.
- **http-uri**
  Specifies that HTTP URIs should be modified.
- **http-host**
  Specifies that HTTP hosts should be modified.
- **http-header**
  Specifies that HTTP headers should be modified.
- **http-referer**
  Specifies that HTTP referers should be modified.
- **http-cookie**
  Specifies that HTTP cookies should be modified.
- **http-set-cookie**
  Specifies that HTTP set cookies should be modified.
- **http-reply**
  Specifies that HTTP replies should be modified.
- **log**
  Specifies that a log should be generated.
- **pem**
  Specifies that the Policy Enforcement Manager should be applied.
- **cache**
  Specifies that the cache should be modified.
- **compress**
  Specifies that compression should be modified.
- **decompress**
  Specifies that decompression should be modified.
- **forward**
  Specifies that forwarding should be modified.
- **tcp-nagle**
  Specifies that TCP nagling rules should be modified.
- **wam**
  Specifies that the Acceleration Module should be invoked.
- **asm**
  Specifies that the Application Security Manager should be invoked.
- **l7dos**
  Specifies that a Layer 7 DOS protection policy should be invoked.
- **avr**
  Specifies that Application Visibility Reporting should be invoked.
- **tcl**
  Specifies that a TCL script should be invoked.

  - **response-adapt**
    Specifies that response adaptation should be invoked.
  - **request-adapt**
    Specifies that request adaptation should be invoked.
  - **server-ssl**
    Specifies that a Server SSL profile should be invoked.
- **strategy**
  Specifies the match strategy to use for this policy. May either be a system provided stratgey or a user created one.

See Also

create, *delete*, *edit*, glob, *list*, *modify*, *policy-strategy*, regex, *reset-stats*, *show*, *tmsh*

policy-strategy

Configures a policy-strategy for Centralized Policy Manager.

Syntax

Modify the policy-strategy component within the **ltm** module using the syntax shown in the following sections.

For additional it's details, refer to Local Traffic Policy documentation on the AskF5 knowledge base at http://support.f5.com.

Create/Modify

```
create policy-strategy [name]
modify policy-strategy [name]
  [ strategy | [ all-match | best-match | first-match ] ]
  operands [add | delete | modify | replace-all-with] {
        [ [integer] ] {
           all | http-header | password | tcp | app-service | http-host |
           pathtext | cipher | http-method | path-segment |
           unnamed-query-parameter | cipher-bits | http-referer | port |
           username | client-ssl | http-set-cookie | protocol | value | code |
           http-status | query-parameter | version | domain | http-uri |
           query-string | vlan | expiry | http-version | request | vlan-id |
           extension | major | response | host | minor | route-domain |
           http-basic-auth | mss | rtt | http-cookie | name | scheme
          }
    }
```

Display

```
list policy-strategy
list policy-strategy [ [ [name] | [glob] | [regex] ] ... ]
  all-properties
  non-default-properties
  one-line
  partition
show policy-strategy
show policy-strategy [name]
  all-properties
  (default | exa | gig | kil | meg | peta | raw | tera | yotta | zetta)
  detail
  field-fmt
```

Delete

```
delete policy-strategy [name]
```

Description

You can use this **policy-strategy** component to configure a user defined matching strategy for centralized policies.

Examples

create policy-strategy my_strategy strategy first-match

Creates the policy strategy **my_strategy** which matches the first rule selected.

Options

- **app-service**
  Specifies the name of the application service to which the policy strategy belongs. The default value is **none**. **Note:** If the **strict-updates** option is **enabled** on the application service that owns the object, you cannot modify or delete the policy strategy. Only the application service can modify or delete the policy strategy.
- **description**
  User defined description.
- **operands**
  Specifies the attribute for the rule to match. Sometimes this represents a specific value (for example, http-method or http-status), but frequently the operand needs a specific Selector to identify an instance (for example, http-header needs a Selector name parameter). Note: This option is only valid if best-match is selected as the strategy to use.
  - **all**
    Select all attributes.
  - **http-header**
    Specifies to select when an HTTP header is processed.
  - **password**
    Specifies to select when a password is discovered.
  - **tcp**
    Specifies to select when a TCP connection is processed.
  - **app-service**
    Specifies the name of the application service to which the operand belongs. The default value is **none**. **Note:** If the **strict-updates** option is **enabled** on the application service that owns the object, you cannot modify or delete the operand. Only the application service can modify or delete the operand.
  - **http-host**
    Specifies to select when an HTTP host is processed.
  - **path**
    Specifies to select when a path is matched.
  - **text**
    Specifies to select when text is matched.
  - **cipher**
    Specifies to select when a cipher is matched.
  - **http-method**
    Specifies to select when an HTTP method is processed.

- **path-segment**
  Specifies to select when a path segment is matched.
- **unnamed-query-parameter**
  Specifies to select when a unnamed query parameter is matched.
- **cipher-bits**
  Specifies to select when cipher bits are matched.
- **http-referer**
  Specifies to select when an HTTP referer is processed.
- **port**
  Specifies to select when cipher bits are matched.
- **username**
  Specifies to select when a username is matched.
- **client-ssl**
  Specifies to select when a client SSL is matched.
- **http-set-cookie**
  Specifies to select when an HTTP set cookie is processed.
- **protocol**
  Specifies to select when a protocol is matched.
- **value**
  Specifies to select when a value is matched.
- **code**
  Specifies to select when a code is matched.
- **http-status**
  Specifies to select when an HTTP status cookie is processed.
- **query-parameter**
  Specifies to select when a query parameter is matched.
- **version**
  Specifies to select when a version is matched.
- **domain**
  Specifies to select when a domain is matched.
- **http-uri**
  Specifies to select when an HTTP URI is processed.
- **query-string**
  Specifies to select when a query string is matched.
- **vlan**
  Specifies to select when a VLan is matched.
- **expiry**
  Specifies to select when an expiry is matched.
- **http-version**
  Specifies to select when an HTTP Version is processed.
- **request**
  Specifies to select when the value selected is on request.
- **vlan-id**
  Specifies to select when a VLan ID is matched.

- **extension**
  Specifies to select when a VLan ID is matched.
- **major**
  Specifies to select when a major is matched.
- **response**
  Specifies to select when the value selected is on response.
- **host**
  Specifies to select when a host is matched.
- **minor**
  Specifies to select when a minor is matched.
- **route-domain**
  Specifies to select when a route domain is matched.
- **http-basic-auth**
  Specifies to select when an HTTP Basic Authorization is processed.
- **mss**
  Specifies to select when a maximum segment size is matched.
- **rtt**
  Specifies to select when a round trip time is matched.
- **http-cookie**
  Specifies to select when an HTTP Basic Cookie is processed.
- **name**
  Specifies to select when a name is matched.
- **scheme**
  Specifies to select when a scheme is matched.

◆ **strategy**
Specifies the match method: all-match, best-match, or first-match. On all-match, all matched rules are returned to be processed. When best-match is selected, the best match as determined by the operands determines the the value selected. When first-match is selected, the value selected from the first matched rule (by precedence) is matched.

See Also

create, *delete*, *edit*, glob, *list*, *modify*, *policy*, regex, *reset-stats*, *show*, *tmsh*

pool

Configures load balancing pools for the Local Traffic Manager.

Syntax

Modify the pool component within the **ltm** module using the syntax shown in the following sections.

Create/Modify

```
create pool [name]
modify pool [name]
  all
  allow-nat [yes | no]
  allow-snat [yes | no]
  app-service [[string] | none]
  description [string]
  gateway-failsafe-device [string]
  ignore-persisted-weight [yes | no]
  ip-tos-to-client [pass-through | [integer] ]
  ip-tos-to-server [pass-through | [integer] ]
  link-qos-to-client [pass-through | [integer] ]
  link-qos-to-server [pass-through | [integer] ]
  load-balancing-mode [dynamic-ratio-member | dynamic-ratio-node |
                       fastest-app-response | fastest-node |
                       least-connections-members |
                       least-connections-node |
                       least-sessions |
                       observed-member | observed-node |
                       predictive-member | predictive-node |
                       ratio-least-connections-member |
                       ratio-least-connections-node |
                       ratio-member | ratio-node | ratio-session |
                       round-robin | weighted-least-connections-member |
                       weighted-least-connections-node]
  members [add | delete | modify | replace-all-with] {
     [ [node_name:port] ] {
        address [ip address]
        app-service [[string] | none]
        connection-limit [integer]
        description [string]
        dynamic-ratio [integer]
        inherit-profile [enabled | disabled]
        logging [enabled | disabled]
        monitor [name]
        priority-group [integer]
        profiles [none | profile_name]
        rate-limit [integer]
        ratio [integer]
        session [user-enabled | user-disabled]
        state [ user-up | user-down ]
         fqdn {
             name [string]
             address-family [ipv4 | ipv6]
             autopopulate [enabled | disabled]
             down-interval [integer]
```

```
            interval [integer]
          }
       }
    }
    members none
    metadata
      [add | delete | modify] {
        [metadata_name ... ] {
          value [ "value content" ]
          persist [ true | false ]
        }
    }
    min-active-members [integer]
    min-up-members [integer]
    min-up-members-action [failover | reboot | restart-all]
    min-up-members-checking [enabled | disabled]
    monitor [name]
    profiles [none | profile_name]
    queue-on-connection-limit [enabled | disabled]
    queue-depth-limit [integer]
    queue-time-limit [integer]
    reselect-tries [integer]
    service-down-action [drop | none | reselect | reset]
    slow-ramp-time [integer]
edit pool [ [ [name] | [glob] | [regex] ] ... ]
    all-properties
    non-default-properties
reset-stats pool
reset-stats pool [ [ [name] | [glob] | [regex] ] ... ]
mv pool [ [[source-name] [destination-name]] | [[name] to-folder [folder-name]] |
[[name...name] to-folder [folder-name]] ]
    to-folder
```

Display

```
list pool
list pool [ [ [name] | [glob] | [regex] ] ... ]
show running-config pool
show running-config pool [ [ [name] | [glob] | [regex] ] ... ]
  all-properties
  non-default-properties
  one-line
  partition
show pool
show pool [name]
  all-properties
  (default | exa | gig | kil | meg | peta | raw | tera | yotta | zetta)
  detail
  field-fmt
```

Delete

```
delete pool [name]
```

◆ Note

You must remove all references to a pool before you can delete the pool.

Description

You can use this **pool** component to configure the pool definitions on the Local Traffic Manager. A load balancing pool is a logical set of devices, such as Web servers, that you group together to receive and process traffic.

Examples

create pool my_pool members add { member 10.2.3.11:http member 10.2.3.12:http }

Creates a Local Traffic Manager pool named **my_pool** with two members, **10.2.3.11** and **10.2.3.12**, using the default values for the pool and pool members.

delete pool my_pool

Deletes the pool named **my_pool**.

show pool

Displays statistics and status for all Local Traffic Manager pools in the system configuration.

show pool all-properties

Displays statistics and status for all Local Traffic Manager pools in the system configuration.

Note that if the system includes Packet Velocity® ASIC (PVA) and PVA Assist capabilities, this command displays status and statistics for that feature.

list pool my_pool

Displays properties of the pool named **my_pool**.

mv /ltm pool /Common/my_pool to-folder /Common/some_folder

Moves an LTM pool named **my_pool** and all of its Pool Members to the folder named **some_folder**, where **some_folder** has already been created under **/Common**.

Please refer to the **mv** manual page for additional examples on how to use the mv command.

Options

- **all**
  Specifies that you want to modify all of the existing components of the specified type.
- **allow-nat**
  Specifies whether the pool can load balance network address translation (NAT) connections. The default value is **yes**.
- **allow-snat**
  Specifies whether the pool can load balance secure network address translation (SNAT) connections. The default value is **yes**.

- **app-service**
  Specifies the name of the application service to which the pool belongs. The default value is **none**. **Note:** If the **strict-updates** option is **enabled** on the application service that owns the object, you cannot modify or delete the pool. Only the application service can modify or delete the pool.
- **description**
  User defined description.
- **gateway-failsafe-device**
  Specifies that the pool is a gateway failsafe pool in a redundant configuration. The gateway-failsafe-device identifies the device that depends on the gateway. If the monitor associated with the pool reports that the gateway is down, the device goes to the standby state. The default value for this string is empty, the feature is not configured.
- **glob**
  Displays the items that match the **glob** expression. See **help glob** for a description of **glob** expression syntax.
- **ignore-persisted-weight**
  Discounts the weight of connections made to pool members selected through persistence, rather than as a result of the algorithm configured on the pool. If the connection's weight is ignored, then it is not treated as a 'pick' for that pool member, and does not influence subsequent pool member load balancing decisions.
  This option only impacts pools configured with one of the following load balancing modes: **observed-member**, **observed-node**, **predictive-member**, **predictive-node**, **ratio-least-connections-member**, **ratio-least-connections-node**, **ratio-member**, or **ratio-node**.
  The default value is **no**, which results in persisted pool member connections being accounted for during load balancing calculations.
- **ip-tos-to-client**
  Specifies the Type of Service (ToS) level to use when sending packets to a client. The default value is **65535** (pass-through).
- **ip-tos-to-server**
  Specifies the ToS level to use when sending packets to a server. The default value is **65535** (pass-through).
- **link-qos-to-client**
  Specifies the Link Quality of Service (QoS) level to use when sending packets to a client. The default value is **65535** (pass-through).
- **link-qos-to-server**
  Specifies the Link QoS level to use when sending packets to a server. The default value is **65535** (pass-through).
- **load-balancing-mode**
  Specifies the modes that the system uses to load balance name resolution requests among the members of this pool. The default value is **round-robin**.
  The options are:

- **dynamic-ratio-member**
  Specifies that the system distributes connections based on various aspects of real-time server performance analysis, such as the number of current connections per node or the fastest node response time. This mode is similar to the **dynamic-ratio-node** mode, except that weights are based on continuous monitoring of the servers and are therefore continually changing.
- **dynamic-ratio-node**
  Specifies that the system distributes connections based on various aspects of real-time server performance analysis, such as the number of current connections per node or the fastest node response time. This mode is similar to the **dynamic-ratio-member** mode, except that weights are based on continuous monitoring of the servers and are therefore continually changing.
- **fastest-app-response**
  Specifies that the system passes a new connection based on the fastest response of all currently active nodes in a pool. This mode might be particularly useful in environments where nodes are distributed across different logical networks.
- **fastest-node**
  Specifies that the system passes a new connection based on the fastest response of all pools of which a server is a member. This mode might be particularly useful in environments where nodes are distributed across different logical networks.
- **least-connections-member**
  Specifies that the system passes a new connection to the node that has the least number of current connections in the pool. This mode works best in environments where the servers or other equipment you are load balancing have similar capabilities.
  This dynamic load balancing mode distributes connections based on various aspects of real-time server performance analysis, such as the current number of connections per node or the fastest node response time.
- **least-connections-node**
  Specifies that the system passes a new connection to the node that has the least number of current connections out of all pools of which a node is a member. This mode works best in environments where the servers or other equipment you are load balancing have similar capabilities.
  This dynamic load balancing mode distributes connections based on various aspects of real-time server performance analysis, such as the number of current connections per node, or the fastest node response time.
- **least-sessions**
  Specifies that the system passes a new connection to the node that has the least number of current sessions. This mode works best in environments where the servers or other equipment you are load balancing have similar capabilities.

This dynamic load balancing mode distributes connections based on various aspects of real-time server performance analysis, such as the number of current sessions.

- **observed-member**
  Specifies that the system ranks nodes based on the number of connections. Nodes that have a better balance of fewest connections receive a greater proportion of the connections.
  This mode differs from the **least-connections-member** mode, which measures connections only at the moment of load balancing, while the **observed-member** mode tracks the number of Layer 4 connections to each node over time and creates a ratio for load balancing.
  This dynamic load balancing mode works well in any environment, but may be particularly useful in environments where node performance varies significantly.
- **observed-node**
  Specifies that the system ranks nodes based on the number of connections. Nodes that have a better balance of fewest connections receive a greater proportion of the connections.
  This mode differs from **least-connections-node** mode, which measures connections only at the moment of load balancing, while the **observed-node** mode tracks the number of Layer 4 connections to each node over time and creates a ratio for load balancing.
  This dynamic load balancing method works well in any environment, but may be particularly useful in environments where node performance varies significantly.
- **predictive-member**
  Uses the ranking method used by the **observed-member** mode, except that the system analyzes the trend of the ranking over time, determining whether a node's performance is improving or declining. The nodes in the pool with better performance rankings that are currently improving, rather than declining, receive a higher proportion of the connections. This dynamic load balancing mode works well in any environment.
- **predictive-node**
  Uses the ranking method used by the **observed-node** mode, except that the system analyzes the trend of the ranking over time, determining whether a node's performance is improving or declining. The nodes in the pool with better performance rankings that are currently improving, rather than declining, receive a higher proportion of the connections. This dynamic load balancing mode works well in any environment.
- **ratio-least-connections-member**
  Specifies that the system weights connections to each pool member based on the value of the ratio weight defined for each pool member. If a ratio weight is unspecified, it will be treated as a default value of '1'.

- **ratio-least-connections-node**
  Specifies that the system weights connections to each pool member based on the value of the ratio weight defined for the pool member's node. If a ratio weight is unspecified, it will be treated as a default value of '1'.
- **ratio-member**
  Specifies that the number of connections that each machine receives over time is proportionate to a ratio weight you define for each machine within the pool.
- **ratio-node**
  Specifies that the number of connections that each machine receives over time is proportionate to a ratio weight you define for each machine across all pools of which the server is a member.
- **ratio-session**
  Specifies that the number of sessions that each machine receives over time is proportionate to a ratio weight that you define for each machine within the pool.
- **round-robin**
  Specifies that the system passes each new connection request to the next server in line, eventually distributing connections evenly across the array of machines being load balanced. This mode works well in most configurations, especially if the equipment that you are load balancing is roughly equal in processing speed and memory.
- **weighted-least-connections-member**
  Specifies that the system passes a new connection to the pool member that is handling the lowest percentage of the specified maximum number of concurrent connections allowed. This mode works best in environments where the servers or other equipment you are load balancing have different but quantified capability limits.
  This mode requires that you specify a value for the **connection-limit** option for all members of the pool, but does not require all servers or other equipment you are load balancing to have similar capabilities.
- **weighted-least-connections-node**
  Specifies that the system passes a new connection to the node that is handling the lowest percentage of the specified connection limit. This mode works best in environments where the servers or other equipment you are load balancing have different but quantified capability limits.
  This mode requires that you specify a value for the **connection-limit** option for all nodes, but does not require all servers or other equipment you are load balancing to have similar capabilities.

◆ **members**
Adds, deletes, or replaces a set of pool members, by specifying a node name and service port in the format **[node name/port]**. If a node by the specified name does not exist, it will be created. You can configure the following options for a pool member:

- **address**
  Specifies the IP address of a pool member if a node by the name specified does not already exist.

- **app-service**
  Specifies the name of the application service to which the pool member belongs. The default value is **none**. **Note:** If the **strict-updates** option is **enabled** on the application service that owns the object, you cannot modify or delete the pool member. Only the application service can modify or delete the pool member.
- **connection-limit**
  Specifies the maximum number of concurrent connections allowed for a pool member. The default value is **0** (zero).
- **description**
  User defined description.
- **dynamic-ratio**
  Specifies a range of numbers that you want the system to use in conjunction with the ratio load balancing method. The default value is **1**.
- **fqdn**
  Specifies the attributes for defining a fully qualified domain name for the node.
  - **name**
    Specifies the fully-qualified domain name of the node.
  - **address-family**
    Specifies whether the fqdn should consider IPv4, IPv6, or IP-agnostic address family.
  - **autopopulate**
    Specifies whether a node defined by a fully-qualified domain name should automatically scale to the set of IP addresses returned by the DNS query. If **disabled**, only one ephemeral node is generated from the first IP address returned by DNS. The default is **disabled**.
  - **interval**
    Specifies the interval to instantiate DNS queries on a fully-qualified domain name. The default is the TTL.
  - **down-interval**
    Specifies the interval for the domain name resolution operation when a DNS query fails.
- **inherit-profile**
  Specifies whether the pool member inherits the encapsulation profile from the parent pool. The default value is **enabled**. If you disable inheritance, no encapsulation takes place, unless you specify another encapsulation profile for the pool member using the **profiles** attribute.
- **logging**
  Specifies whether the monitor applied should log its actions. Logs are stored in /var/log/monitors/ and are regularily rotated and compressed. The default value is **disabled**. This option isn't a part of configuration and will reset to **disabled** on load. This option doesn't sync.

- **monitor**
  Specifies the health monitors that are configured to monitor the pool member. The default value is **default**, the system monitors the pool member using the monitors specified for the pool.
  You can specify:
  - A single monitor, for example, **modify pool mypool members modify { pool_member_1:80 { monitor http } }**.
  - Multiple monitors, for example, **modify pool mypool members modify { pool_member_1:80 { monitor http and https } }**.
  - A minimum number of monitors, for example, **modify pool mypool members modify { pool_member_1:80 { monitor min 1 of { http https } } }**.
  - No monitor rule or remove a monitor rule, for example, **modify pool mypool members modify { pool_member_1:80 { monitor none } }**.
- **profiles**
  Specifies the encapsulation profile to use for the pool member, when the **inherit-profile** attribute is disabled. The default value is **none**.
- **priority-group**
  Specifies the priority group within the pool for this pool member. Valid values are **0** through **65535**. The system sends traffic to groups in order of priority. The default value is **0**.
- **rate-limit**
  Specifies the maximum number of connections per second allowed for a pool member. The default value is ‘disabled’.
- **ratio**
  Specifies the weight of the pool member for load balancing purposes. The default value is **1**.
- **session**
  Establishing a session with a pool member is establishing the ability of the client to persist to the pool member when making new connections. When a pool member is session disabled, clients that have already established sessions with the pool member may create new connections, but a client that has not already established a session may not create a new one (or make a connection which would create a new session). This feature is used to gently drain connections from a node, typically as part of a maintenance operation. The default value is **user-enabled**.
  The value of this property can be set by system or by user. If the value is set by system, the property will not be displayed in "Edit" command. But, users can add this field in if they need to modify this property. The values which user can set for this property are **user-enabled** and **user-disabled**.

- **state**
  Marks the pool member **user-up** or **user-down**. The default value is **user-up**.

- **metadata**
  Associates user-defined data, each of which has name and value pair and persistence. The default value is **persistent**, which saves the data to the config file.
- **min-active-members**
  Specifies the minimum number of members that must be **up** for traffic to be confined to a priority group when using priority-based activation. The default value is **0** (zero). An active member is a member that is **up** (not marked down) and is handling fewer connections than its connection limit.
- **min-up-members**
  Specifies the minimum number of pool members that must be **up**; otherwise, the system takes the action specified in the **min-up-members-action** option.
  Use this option for gateway pools in a redundant system where a unit number is applied to the pool. This indicates that the pool is configured only on the specified unit.
- **min-up-members-action**
  Specifies the action to take if **min-up-members-checking** is **enabled**, and the number of active pool members falls below the number specified in the **min-up-members** option. The default value is **failover**. The options are:
  - **reboot**
    Specifies that when the **min-up-members-checking** option is **enabled**, and the number of active pool members is less than the number specified in the **min-up-members** option, the system restarts.
  - **restart-all**
    Specifies that when the **min-up-members-checking** option is **enabled**, and the number of active pool members is less than the number specified in the **min-up-members** option, the system restarts.
  - **failover**
    Specifies, for a redundant system, that when the **min-up-members-checking** option is **enabled**, and the number of active pool members is less than the number specified in the **min-up-members** option, the system fails over.
- **min-up-members-checking**
  Enables or disables the **min-up-members** feature. If you enable this feature, you must also specify a value for both the **min-up-members** and **min-up-members-action** options.
- **monitor**
  Specifies the health monitors that the system uses to determine whether it can use this pool for load balancing. The monitor marks the pool **up** or **down** based on whether the monitor is successful. The default value is **none**.
  You can specify:

- A single monitor, for example, **modify pool mypool monitor http**.
- Multiple monitors, for example, **modify pool mypool monitor http and https**.
- A minimum number of monitors, for example, **modify pool mypool monitor min 1 of {http and https}**.
- No monitor rule or remove a monitor rule, for example, **modify pool mypool monitor none**.

◆ **name**
Specifies a unique name for the component. This option is required for the commands **create**, **delete**, and **modify**.

◆ **partition**
Displays the administrative partition within which the pool resides.

◆ **profiles**
Specifies the profile to use for encapsulation. The default value is **none**, which indicates no encapsulation.

◆ **regex**
Displays the items that match the regular expression. The regular expression must be preceded by an at sign (@[regular expression]) to indicate that the identifier is a regular expression. See **help regex** for a description of regular expression syntax.

◆ **reselect-tries**
When set to the default value of **0** (zero) the system does not attempt to load balance to another pool member after a passive failure. A passive failure is a pool member connection failure.
When set to any other value, the system attempts to load balance to another pool member after a passive failure, and if that attempt also results in a passive failure, the system repeats the process until the specified number of reselection tries is reached.

◆ **reset-stats**
Resets the statistics for the specified component to **0** (zero).

◆ **service-down-action**
Specifies the action to take if the service specified in the pool is marked **down**. The options are:

- **drop**
  Specifies that the system drops connections when a the service is marked **down**.
- **none**
  Specifies that the system takes no action when a the service is marked **down**. This is the default value.
- **reselect**
  Specifies that the system reselects a node for the next packet that comes in on a Layer 4 connection, if the service of the existing connection is marked **down**.

- **reset**
  Specifies that the system resets when a the service is marked **down**.

- **slow-ramp-time**
  Specifies, in seconds, the ramp time for the pool. This provides the ability to cause a pool member that has just been **enabled**, or marked **up**, to receive proportionally less traffic than other members in the pool. The proportion of traffic the member accepts is determined by how long the member has been up in comparison to the value of the **slow-ramp-time** option for the pool.
  For example, if the **load-balancing-mode** of a pool is **round-robin** and it has a **slow-ramp-time** of **60** seconds, when a pool member has been up for only 30 seconds, the pool member receives approximately half the amount of new traffic as other pool members that have been up for more than 60 seconds. After the pool member has been up for 45 seconds, it receives approximately three quarters of the new traffic.
  The **slow-ramp-time** option is particularly useful when used with the **least-connections-member** load balancing mode. The default value is **10**.

- **to-folder**
  This is used with the **mv** command to specify a **folder** in which to move the **pool** and its **members** to.

◆ Note

pools *can be moved to any folder under* ***/Common****, but dependencies upon it may restrict moving it out of* ***/Common***.

See Also

create, *delete*, *edit*, glob, *list*, *modify*, *mv*, *virtual*, regex, *reset-stats*, *show*, *tmsh*

rule

Configures an iRule for traffic management system configuration.

Syntax

Configure the **rule** component within the **ltm** module using the syntax shown in the following sections.

Create/Modify

```
create rule [name]
edit rule [name]
modify rule [ [ [name] | [glob] | [regex] ] ... ]
```

◆ Note

*When using tmsh, you can only create iRules using the editor, which starts when you use the create or edit commands. You cannot create an iRule directly on the command line. The vim editor applies the autoindent and smartindent options. You can toggle on/off paste mode using the **F12** key.*

◆ Note

You can also edit user metadata associated with an iRule. See the example section for more information.

Display

```
list rule
list rule [ [ [name] | [glob] | [regex] ] ... ]
show running-config rule
show running-config rule [ [ [name] | [glob] | [regex] ] ... ]
    all-properties
    non-default-properties
show rule
show rule [ [ [name] | [glob] | [regex] ] ... ]
    (default | exa | gig | kil | meg | peta | raw | tera | yotta | zetta)
    field-fmt
mv rule [ [[source-name] [destination-name]] | [[name] to-folder [folder-name]] |
[[name...name] to-folder [folder-name]] ]
    to-folder
```

Delete

```
delete rule [name]
```

Generate

```
generate rule [name]
    checksum
    signature
```

Description

You cannot edit the system rules that come with the BIG-IP system. However, you can open a system rule in the editor and use it as a template to create a new rule.

To create a new rule using a system rule as a template:

1. Enter the command sequence **edit rule [system rule name]**.
   tmsh opens the system rule in an editor.
2. Change the name of the rule in the editor.
3. Edit the rule and exit the editor.
   tmsh checks for syntax errors, and if there are none, it saves the new rule.

For more information about iRules®, see **http://devcentral.f5.com/**.

Examples

list rule

Displays all iRules.

delete rule my_irule

Deletes the iRule named **my_irule**.

rule my_irule {
  when RULE_INIT {
  }
  priority 1

```
when SERVER_CONNECTED {
}
timing on
check strict
}
```

Creates an iRule named **my_irule**.

generate rule my_irule checksum

Generates a checksum for the rule definition and adds the checksum to the rule.

generate rule my_irule signature signing-key my_key

Generates a signature for the rule definition using the specified private key and adds the signature to the rule.

Note: For a rule that includes a checksum or signature to successfully load, the rule definition contents must match the stored checksum or signature. To modify the rule definition and still retain the checksum or signature, the **ignore-verification** attribute must be set to **true**. This is done by editing the rule and adding the **ignore-verification** attribute, which allows the modified rule to load and changes the verification status to **Not Verified**:

```
rule my_irule {
   when RULE_INIT {}
   definition-checksum 7c0dba9aa53e8959042c6cfe041d3d11
   ignore-verification true
}
```

Modifies an existing iRule named **my_irule** by adding a new metadata and modifying an existing metadata:

```
modify rule my_irule {
   when RULE_INIT {}
   definition-checksum 7c0dba9aa53e8959042c6cfe041d3d11
   metadata replace-all-with {
      my_meta {
persist false
            value "hello"
      }
      my_meta2 {
persist false
            value "hello 2"
      }
   }
}
```

The metadata attribute is the user defined key/value pair. Metadata has the following format:

```
metadata
  [add | delete | modify] {
   [metadata_name] {
   value [ "value content" ]
   persist [ true | false ]
  }
}>
```

Deletes a metadata from an iRule:

```
modify rule my_irule {
   when RULE_INIT {}
   definition-checksum 7c0dba9aa53e8959042c6cfe041d3d11
   metadata delete { my_meta }
}
```

mv /ltm rule /Common/my_rule to-folder /Common/some_folder

Moves an iRule named **my_rule** to the folder named **some_folder**, where **some_folder** has already been created under **/Common**.

◆ Note

Please note that you may not move an iRule that has an explicit usage of a configuration object, such as a pool.

Options

- **checksum**
  Generates a checksum for the rule definition and adds the checksum to the rule. This option is used only with the **generate** command.
- **glob**
  Displays the items that match the **glob** expression. See **help glob** for a description of **glob** expression syntax.
- **name**
  Specifies a unique name for the component. This option is required for the **create**, **delete**, and **modify** commands.
- **regex**
  Displays the items that match the regular expression. The regular expression must be preceded by an at sign (@[regular expression]) to indicate that the identifier is a regular expression. See **help regex** for a description of regular expression syntax.
- **signature**
  Generates a signature for the rule definition using the specified private key and adds the signature to the rule as a property. This option is used only with the **generate** command.
- **signing-key**
  Specifies the private key to use for signing the rule. This is used only with the **signature** option.
- **meta-data**
  Specifies the user-defined key/value pair associated with the rule. See the example section for usage format.

See Also

create, *delete*, *edit*, *generate*, glob, *list*, *modify*, *mv*, regex, *show*, *tmsh*

snat

Configures secure network address translation (SNAT).

Syntax

Configure the **snat** component within the **ltm** module using the syntax shown in the following sections.

Create/Modify

```
create snat [name]
modify snat [name]
    (automap | none)
    auto-lasthop [default | enabled | disabled ]
    app-service [[string] | none]
    description [string]
    mirror { [disabled | enabled | none] }
    origins
      [add  | delete |  replace-all-with] {
        [address ... | address/mask ... ]
    }
    snatpool [ name ]
    source-port [change | preserve | preserve-strict ]
    translation [translation name ... ]
    vlans
      [add  | delete |  replace-all-with] {
        [vlan name ... ]
    }
    vlans [ default | none]
    [vlans-disabled | vlans-enabled ]
    metadata
      [add | delete | modify] {
        [metadata_name ... ] {
          value [ "value content" ]
          persist [ true | false ]
        }
    }
edit snat [ [ [name] | [glob] | [regex] ] ... ]
    all-properties
    non-default-properties
```

Display

```
list snat
list snat [ [ [name] | [glob] | [regex] ] ... ]
show running-config snat
show running-config snat [ [ [name] | [glob] | [regex] ] ... ]
    all-properties
    non-default-properties
    one-line
show snat
show snat [ [ [name] | [glob] | [regex] ] ... ]
    (default | exa | gig | kil | meg | peta | raw | tera | yotta | zetta)
    detail
    field-fmt
```

Delete

```
delete snat [name]
```

Description

You can use the **snat** component to configure a SNAT. A SNAT defines the relationship between an externally visible IP address, SNAT IP address, or translated address, and a group of internal IP addresses, or originating addresses, of individual servers at your site.

Examples

create snat my_snat origins add { 10.1.1.3 } translation mySnatTranslation

Creates the SNAT **my_snat** that translates the address of connections that originate from the address **10.1.1.3** to the translation address **mySnatTranslation**.

list snat all-properties

Displays all properties for all SNATs.

Options

- **automap**
  Specifies that the system translates the source IP address to an available self IP address when establishing connections through the virtual server. You can use this option only if you do not use the **snatpool** and **translation** options.
  Note that when you use the **edit** command to create a new snat, by default automap is **enabled**. If you do not want to use automap, you must turn this feature off by using the **none** option.
- **app-service**
  Specifies the name of the application service to which this object belongs. The default value is **none**. **Note:** If the **strict-updates** option is **enabled** on the application service that owns the object, you cannot modify or delete this object. Only the application service can modify or delete this object.
- **description**
  User defined description.
- **glob**
  Displays the items that match the **glob** expression. See **help glob** for a description of **glob** expression syntax.
- **mirror**
  Enables or disables mirroring of SNAT connections. The default value is **none**.

- **name**
  Specifies a unique name for the component. This option is required for the commands **create**, **delete**, and **modify**.
- **origins**
  Specifies a set of IP addresses and subnets from which connections originate. This option is required.
- **regex**
  Displays the items that match the regular expression. The regular expression must be preceded by an at sign (@[regular expression]) to indicate that the identifier is a regular expression. See **help regex** for a description of regular expression syntax.
- **snatpool**
  Specifies the name of a SNAT pool. You can only use this option if you do not use the **automap** and **translation** options.
- **source-port**
  Specifies whether the system preserves the source port of the connection. The default value is **preserve**.
  The options are:
  - **change**
    Use this setting to obfuscate internal network addresses.
  - **preserve**
    Specifies to preserve the source port of the connection.
  - **preserve-strict**
    Use this value only for UDP under very special circumstances such as nPath or transparent (that is, no translation of any other L3/L4 field), where there is a 1:1 relationship between virtual IP addresses and node addresses, or when clustered multi-processing (CMP) is disabled.
- **translation**
  Specifies the name of a translated IP address. Note that translated addresses are outside the traffic management system. You can use this option only if you do not use the **automap** and **snatpool** options.
- **vlans**
  Specifies the name of the VLAN to which you want to assign the SNAT. The default value is **none**.
- **vlans-disabled**
  Disables the SNAT on all VLANs. This is the default value.
- **vlans-enabled**
  Enables the SNAT on all VLANs.
- **metadata**
  Associates user defined data, each of which has name and value pair and persistence. Persistent(default) means the data will be saved into config file.

See Also

create, *delete*, *edit*, glob, *list*, *snat-translation*, *snatpool*, *modify*, regex, *show*, *tmsh*

snat-translation

Configures an explicit secure network address translation (SNAT) translation address.

Syntax

Configure the **snat-translation** component within the **ltm** module using the syntax shown in the following sections.

Create/Modify

```
create snat-translation [all | [name] ]
modify snat-translation [all | [name] ]
    address [ip address]
    arp [disabled | enabled]
    app-service [[string] | none]
    connection-limit [integer]
    description [string]
    [disabled | enabled]
    ip-idle-timeout [indefinite | [integer] ]
    tcp-idle-timeout [indefinite | [integer] ]
    udp-idle-timeout [indefinite | [integer] ]
    traffic-group [[string] | default | non-default | none]
edit snat-translation [ [ [name] | [glob] | [regex] ] ... ]
    all-properties
    non-default-properties
```

Display

```
list snat-translation
list snat-translation [ [ [name] | [glob] | [regex] ] ... ]
show running-config snat-translation
show running-config snat-translation [ [ [name] | [glob] | [regex] ] ... ]
    all-properties
    non-default-properties
    one-line
show snat-translation
show snat-translation [ [ [name] | [glob] | [regex] ] ... ]
    (default | exa | gig | kil | meg | peta | raw | tera | yotta | zetta)
    field-fmt
```

Delete

```
delete snat-translation [all | [name] ]
```

Description

Explicitly defines the properties of a SNAT translation address.

Examples

modify snat-translation all arp disabled

Disables Address Resolution Protocol (ARP) on all SNAT translation addresses.

list snat-translation all-properties

Displays all properties of all SNAT translation addresses.

Options

- **address**
  The translation IP address.
- **arp**
  Indicates whether the system responds to ARP requests or sends gratuitous ARPs. The default value is **enabled**.
- **app-service**
  Specifies the name of the application service to which this object belongs. The default value is **none**. **Note:** If the **strict-updates** option is **enabled** on the application service that owns the object, you cannot modify or delete this object. Only the application service can modify or delete this object.
- **connection-limit**
  Specifies the number of connections a translation address must reach before it no longer initiates a connection. The default value of **0** (zero) indicates that the option is **disabled**.
- **description**
  User defined description.
- **disabled**
  Disables SNAT translation.
- **enabled**
  Enables SNAT translation. The default value is **enabled**.
- **glob**
  Displays the items that match the **glob** expression. See **help glob** for a description of **glob** expression syntax.
- **ip-idle-timeout**
  Specifies the number of seconds that IP connections initiated using a SNAT address are allowed to remain idle before being automatically disconnected. The default value is **indefinite**.
- **regex**
  Displays the items that match the regular expression. The regular expression must be preceded by an at sign (@[regular expression]) to indicate that the identifier is a regular expression. See **help regex** for a description of regular expression syntax.

- **tcp-idle-timeout**
  Specifies the number of seconds that TCP connections initiated using a SNAT address are allowed to remain idle before being automatically disconnected. The default value is **indefinite**.
- **udp-idle-timeout**
  Specifies the number of seconds that UDP connections initiated using a SNAT address are allowed to remain idle before being automatically disconnected. The default value is **indefinite**.
- **unit**
  Read-only property that specifies the unit in a redundant system. Derived from **traffic-group**.
- **traffic-group**
  Specifies the traffic group of the failover device group on which the SNAT is active. The default traffic group is inherited from the containing folder.
- **inherited-traffic-group**
  Read-only property that indicates if the **traffic-group** is inherited from the parent folder.

See Also

create, *delete*, *edit*, glob, *list*, *modify*, *snat*, *snatpool*, regex, *show*, *tmsh*

snatpool

Configures a secure network address translation (SNAT) pool.

Syntax

Configure the **snatpool** component within the **ltm** module using the syntax shown in the following sections.

Create/Modify

```
create snatpool [name]
modify snatpool [name]
    app-service [[string] | none]
    description [string]
    members
      [add | delete | replace-all-with] {
        [ip address ... ]
    }
    members [default | none]
edit snatpool [ [ [name] | [glob] | [regex] ] ... ]
    all-properties
    non-default-properties
reset-stats snatpool
reset-stats snatpool [ [ [name] | [glob] | [regex] ] ... ]
```

Display

```
list snatpool
list snatpool [ [ [name] | [glob] | [regex] ] ... ]
show running-config snatpool
show running-config snatpool [ [ [name] | [glob] | [regex] ] ... ]
    all-properties
    non-default-properties
    one-line
show snatpool
show snatpool [ [ [name] | [glob] | [regex] ] ... ]
    (default | exa | gig | kil | meg | peta | raw | tera | yotta | zetta)
    detail
    field-fmt
```

Delete

```
delete snatpool [name]
```

Description

A SNAT pool is a pool of translation addresses that you can map to one or more original IP addresses. Translation addresses in a SNAT pool are not self-IP addresses. You can simply create a SNAT pool and then assign it as a resource directly to a virtual server. This eliminates the need for you to explicitly define original IP addresses to which to map translation addresses.

Examples

create snatpool my_snat_pool1 members add { 11.12.11.24 11.12.11.25 }

Creates the SNAT pool **my_snat_pool1** that contains the translation addresses (members) **11.12.11.24** and **11.12.11.25**.

delete snatpool my_snat_pool1

Deletes the SNAT pool named **my_snat_pool1**.

Options

- **app-service**
  Specifies the name of the application service to which this object belongs. The default value is **none**. **Note:** If the **strict-updates** option is **enabled** on the application service that owns the object, you cannot modify or delete this object. Only the application service can modify or delete this object.
- **description**
  User defined description.
- **glob**
  Displays the items that match the **glob** expression. See **help glob** for a description of **glob** expression syntax.
- **members**
  Specifies translation IP addresses of the pools in the SNAT pool.
- **name**
  Specifies a unique name for the component. This option is required for the commands **create**, **delete**, and **modify**.
- **regex**
  Displays the items that match the regular expression. The regular expression must be preceded by an at sign (@[regular expression]) to indicate that the identifier is a regular expression. See **help regex** for a description of regular expression syntax.

See Also

create, *delete*, *edit*, glob, *list*, *snat*, *snat-translation*, *modify*, regex, *reset-stats*, *show*, *tmsh*

traffic-class

Configures a traffic class.

Syntax

Configure the **traffic-class** component within the **ltm** module using the syntax shown in the following sections.

Create/Modify

```
create traffic-class [name]
modify traffic-class [name]
options:
  app-service [[string] | none]
  classification [string]
  description [string]
  destination-address [ [ip address] | none]
  destination-mask [ [ip address] | none]
  destination-port [ [integer] | [port name] ]
  protocol [any | [protocol] ]
  source-address [ [ip address] | none]
  source-mask [ [ip address] | none]
  source-port [ [integer] | [port name] ]
edit traffic-class [ [ [name] | [glob] | [regex] ] ... ]
    all-properties
    non-default-properties
    one-line
```

Display

```
list traffic-class
list traffic-class [ [ [name] | [glob] | [regex] ] ... ]
show running-config traffic-class
show running-config traffic-class [ [ [name] | [glob] | [regex] ] ... ]
  all-properties
  non-default-properties
  one-line
```

Delete

```
delete traffic-class [name]
```

Description

You can use the **traffic-class** component to configure a traffic class, which is a named group of ports, machines, and subnets. You can then assign this traffic class to a virtual server in order to configure the virtual server to achieve specific Quality of Service (QoS) standards.

Examples

create traffic-class my_traffic_class classification "My traffic class."

Creates a traffic class named **my_traffic_class**, which tags matching flows with the tag **My traffic class**.

list traffic-class all-properties

Displays all of the properties of all of the traffic classes.

delete traffic-class my_traffic_class

Deletes the traffic class named **my_traffic_class**.

Options

- **app-service**
  Specifies the name of the application service to which the traffic class belongs. The default value is **none**. **Note:** If the **strict-updates** option is **enabled** on the application service that owns the object, you cannot modify or delete the traffic class. Only the application service can modify or delete the traffic class.
- **classification**
  Specifies the actual textual tag to be associated with the flow if the traffic class is matched. This option is required.
- **description**
  User defined description.
- **destination-address**
  Specifies destination IP addresses for the system to use when evaluating traffic flow. If traffic flow matches this value, it is tagged with the value in the **classification** option. The default value is **none**.
- **destination-mask**
  Specifies a destination IP address mask for the system to use when evaluating traffic flow. If traffic flow matches this value, it is tagged with the value in the **classification** option. The default value is **none**.
- **destination-port**
  Specifies a destination port for the system to use when evaluating traffic flow. If traffic flow matches this value, it is tagged with the value in the **classification** option. The default value is **0** (zero).
- **glob**
  Displays the items that match the **glob** expression. See **help glob** for a description of **glob** expression syntax.
- **name**
  Specifies a unique name for the component. This option is required for the commands **create**, **delete**, and **modify**.
- **protocol**
  Specifies a protocol for the system to use when evaluating traffic flow. If traffic flow matches this value, it is tagged with the value in the **classification** option. The default value is **any**.

- **regex**
  Displays the items that match the regular expression. The regular expression must be preceded by an at sign (@[regular expression]) to indicate that the identifier is a regular expression. See **help regex** for a description of regular expression syntax.
- **source-address**
  Specifies source IP addresses for the system to use when evaluating traffic flow. If traffic flow matches this value, it is tagged with the value in the **classification** option. The default value is **none**.
- **source-mask**
  Specifies a source IP address mask for the system to use when evaluating traffic flow. If traffic flow matches this value, it is tagged with the value in the **classification** option. The default value is **none**.
- **source-port**
  Specifies a source port for the system to use when evaluating traffic flow. If traffic flow matches this value, it is tagged with the value in the **classification** option. The default value is **0** (zero).

See Also

create, *delete*, *edit*, glob, *list*, *virtual*, *modify*, regex, *tmsh*

virtual

Configures a virtual server.

Syntax

Configure the **virtual** component within the **ltm** module using the syntax shown in the following sections.

Create/Modify

```
create virtual [name]
modify virtual [name]
  all
  address-status [yes | no]
  app-service [[string] | none]
  auth [add | delete | replace-all-with] {
      [profile_name ... ]
  }
  auth [default | none]
  auto-lasthop [default | enabled | disabled ]
  clone-pools [add | delete | replace-all-with] {
      [pool_name ... ] {
        context [clientside | serverside]
      }
  }
  clone-pools none
  cmp-enabled [yes | no]
  connection-limit [integer]
  dhcp-relay
  description [string]
  destination [ [virtual_address_name:port] | [ipv4:port] | [ipv6.port] ]
  [disabled | enabled]
  fallback-persistence [none | [profile name] ]
  flow-eviction-policy [none | [eviction policy name] ]
  fw-enforced-policy [ [policy_name] | none ]
  fw-rules [add | delete | modify | replace-all-with] {
    [ [name] ] {
        action [accept | drop | reject]
        description [string]
        destination {
          address-lists [add | default | delete | replace-all-with] {
            [address list names...]
          }
          address-lists none
          addresses [add | default | delete | replace-all-with] {
            [ [ipv4[/prefixlen] | ipv6[/prefixlen]] ]
          }
          addresses none
          port-lists [add | default | delete | replace-all-with] {
            [port list names...]
          }
          port-lists none
          ports [add | default | delete | none | replace-all-with] {
            [ [port] | [port1-port2] ]
          }
          ports none
```

```
      }
      icmp [add | delete | modify | replace-all-with] {
        [ [icmp_type] | icmp_type:icmp_code ] {
          description [string]
        }
      }
      icmp none
      ip-protocol [protocol name]
      irule [irule name]
      irule-sample-rate [integer]
      log [no | yes]
      place-after [first | last | [rule name]]
      place-before [first | last | [rule name]]
      rule-list [rule list name]
      schedule [schedule name]
      source {
        address-lists [add | default | delete | replace-all-with] {
          [address list names...]
        }
        address-lists none
        addresses [add | default | delete | replace-all-with] {
          [ [ipv4[/prefixlen]] | [ipv6[/prefixlen]] ]
        }
        addresses none
        port-lists [add | default | delete | replace-all-with] {
          [port list names...]
        }
        port-lists none
        ports [add | default | delete | replace-all-with] {
          [ [port] | [port1-port2] ]
        }
        ports none
        vlans [add | default | delete | replace-all-with] {
          [vlan names...]
        }
        vlans none
      }
      status [disabled | enabled | scheduled]
  }
}
fw-rules none
fw-staged-policy [ [policy_name] | none ]
gtm-score [integer]
http-class none
http-class {
  [profile_name ...]
}
ip-forward
ip-protocol [any | [protocol]
internal
l2-forward
last-hop-pool [ [pool_name] | none]
mask { [ipv4] | [ipv6] }
mirror { [disabled | enabled | none] }
nat64 [enabled | disabled]
persist [replace-all-with] {
    [profile_name ... ] {
      default [no | yes]
    }
}
persist none
pool [ [pool_name] | none]
```

```
  profiles [add | delete | replace-all-with] {
      [profile_name ...] {
        context [all | clientside | serverside]
      }
  }
  profiles [default | none]
  rate-class [name]
  rate-limit [integer]
  rate-limit-mode [destination | object | object-destination |
                   object-source | object-source-destination | source |
                   source-destination]
  rate-limit-dst [integer]
  rate-limit-src [integer]
  related-rules { none | [rule_name ...] }
  reject
  rules { [none | [rule_name ... ] }
  snat [automap | none]            DEPRECATED - see source-address-translation
  snatpool [snatpool_name]         DEPRECATED - see source-address-translation
  source { [ipv4[/prefixlen]] | [ipv6[/prefixlen]] }
  source-address-translation {
      pool [ [pool_name] | none]
      type [ automap | lsn | snat | none ]
  }
  source-port [change | preserve | preserve-strict]
  traffic-classes [add | delete | replace-all-with] {
      [traffic_class_name ...]
  }
  traffic-classes [default | none]
  translate-address [enabled | disabled]
  translate-port [enabled | disabled]
  vlans [add | delete | replace-all-with] {
      [vlan_name ... ]
  }
  vlans [default | none]
  vlans-disabled
  vlans-enabled
  metadata [add | delete | modify] {
      [metadata_name ... ] {
        value [ "value content" ]
        persist [ true | false ]
      }
  }
reset-stats virtual [ [ [name] | [glob] | [regex] ] ... ]
  fw-enforced-policy-rules { [rule name] }
  fw-rules  { [rule name] }
  fw-staged-policy-rules  { [rule name] }
  profiles  { [profile name] }
options:
  ip-intelligence-categories
```

Display

```
list virtual
list virtual [ [ [name] | [glob] | [regex] ] ...]
show running-config virtual
show running-config virtual [ [ [name] | [glob] | [regex] ] ... ]
  all-properties
  non-default-properties
  one-line
  partition
```

```
show virtual
show virtual [ [ [name] | [glob] | [regex] ] ... ]
  all-properties (default | exa | gig | kil | meg | peta | raw | tera |
                  yotta | zetta)
  detail
  field-fmt
  ip-intelligence-categories
mv virtual [ [[source-name] [destination-name]] | [[name] to-folder [folder-name]] |
[[name...name] to-folder [folder-name]] ]
  to-folder
```

Delete

```
delete virtual [name]
```

Description

You can use the **virtual** component to create, delete, modify properties on, and display information about virtual servers. Virtual servers are externally visible IP addresses that receive client requests. Rather than sending the requests directly to the destination IP address specified in the packet header, it sends the requests to any of several content servers that make up a load balancing pool. Virtual servers also apply various behavioral settings to multiple traffic types, enable persistence for multiple traffic types, and direct traffic according to user-written iRules®.

◆ Note

*After you configure a Global Traffic Manager listener, when you use the tab completion feature within the **ltm** module, the listener displays as one of the virtual servers in the Configuration Items section.*

Examples

create virtual myV2 { destination 11.11.11.12:any persist replace-all-with { source_addr } } pool myPool}

Creates a virtual server named myV2, which uses the source address persistence method.

modify virtual vs_fl4_http4 profiles replace-all-with { profile-udp }

Replaces the profile associated with the virtual server vs_f14_http4.

◆ Note

To replace the profile associated with a virtual server, you must enclose the name of the new profile in curly brackets.

delete virtual myV4 myV5 myV6

Deletes the virtual servers named myV4, myV5, and myV6.

show virtual myV4

Displays statistics and status for the virtual named **myV4**.

show virtual myV4 all-properties

Displays statistics and status for the virtual named **myV4**.

◆ Note

If the system includes Packet Velocity® ASIC (PVA) and PVA Assist capabilities, this command displays status and statistics for that feature.

mv /ltm virtual /Common/my_vip to-folder /Common/some_folder

Moves a virtual server named **my_vip** to the folder named **some_folder**, where **some_folder** has already been created under **/Common**.

Note: Please note that you may not move a virtual server that is associated with CGNAT configuration items, such as LSN pools.

Options

- **all**
  Specifies that you want to modify all of the existing components of the specified type.
- **address-status**
  Specifies whether the virtual will contribute to the operational status of the associated virtual-address. The default value is 'yes'.
- **app-service**
  Specifies the name of the application service to which the virtual server belongs. The default value is **none**. **Note:** If the **strict-updates** option is **enabled** on the application service that owns the object, you cannot modify or delete the virtual server. Only the application service can modify or delete the virtual server.
- **auth**
  Specifies a list of authentication profile names, separated by spaces, that the virtual server uses to manage authentication.
- **clone-pools**
  Specifies a pool or list of pools that the virtual server uses to replicate either client or server traffic. You must specify a value of either **clientside** or **serverside** for the **context** option for each clone pool. Typically, this option is used for intrusion detection.
- **cmp-enabled**
  Enables or disables clustered multi-processor (CMP) acceleration. This feature applies to certain platforms only. The default value is **yes**.
- **connection-limit**
  Specifies the maximum number of concurrent connections you want to allow for the virtual server. The default value of **0** (zero) allows for an unlimited number of concurrent connections.

- **context**
  Specifies that the pool is either a **clientside** or **serverside** clone pool.

◆ Note

Because validation occurs outside of TMSH, you will receive an error when you modify the context for profiles in a virtual server.

- **dhcp-relay**
  Specifies a virtual server that relays all received dhcp requests to all pool members. If there is no pool, the received request get dropped. If you specify the **dhcp-relay** option, you cannot use the **ip-forward** or **l2-forward** or **reject** options.
- **description**
  User defined description.
- **destination**
  Specifies the name of the virtual address and service on which the virtual server listens for connections.
  The format for "ipv4" is *a*. *b*. *c*. *d* [: *port*]. The format for an "ipv6" address is *a*: *b*: *c*: *d*: *e*: *f*: *g*: *h* [. *port*].
  The default value is **any:any**.
- **(enabled | disabled)**
  Specifies the state of the virtual server. The default value is **enabled**.

◆ Note

*When you disable a virtual server, the virtual server no longer accepts new connection requests. However, it allows current connections to finish processing before going to a **down** state.*

- **fallback-persistence**
  Specifies a fallback persistence profile for the virtual server to use when the default persistence profile is not available. The default value is **none**.
- **flow-eviction-policy**
  Specifies a flow eviction policy for the virtual server to use, to select which flows to terminate when the number of connections approaches the connection limit on the virtual server. The default value is **none**.
- **fw-enforced-policy**
  Specifies an enforced firewall policy. **fw-enforced-policy** rules are enforced on a virtual server as if the policy rules were explicitly defined in the virtual server's **fw-rules**. Either **fw-rules** or **fw-enforced-policy** can be configured on a virtual server, not both of them.
- **fw-enforced-policy-rules**
  Specifies firewall rules enforced on **ltm virtual** via referenced **fw-enforced-policy**.
- **fw-rules**
  Adds, deletes, or replaces a firewall rule. **self-ip** rules are checked when a packet is received that is destined for a **self-ip** /port pair on which there is no **ltm virtual**.

- **action**
  Specifies the action that the system takes when a rule is matched.
  - **accept**
    Specifies that the current packet should be accepted. The packet will be not be compared to any more firewall rules.
  - **drop**
    Specifies that the current packet should be silently dropped. Nothing is sent back to the packet source. The packet is not compared to any other firewall rules.
  - **reject**
    Specifies that the current packet should be dropped. For TCP based protocols a TCP reset is sent to the source. For other protocols **reject** is equivalent to **drop**.
- **description**
  User defined description.
- **destination**
  - **address-lists**
    Specifies a list of address lists (see **security firewall address-list**) against which the packet will be compared.
  - **addresses**
    Specifies a list of addresses and networks against which the packet will be compared.
    The format for "ipv4" is *a*. *b*. *c*. *d* [*/ prefixlen*]. The format for an "ipv6" address is *a*: *b*: *c*: *d*: *e*: *f*: *g*: *h* [*/ prefixlen*].
  - **port-lists**
    Specifies a list of port lists (see **security firewall port-list**) against which the packet will be compared.
  - **ports**
    Specifies a list of ports and port ranges against which the packet will be compared.
- **icmp**
  Specifies a list of ICMP types and codes against which the packet will be compared. The standard integer identifiers are used to specify an ICMP type Example: 3 is destination unreachable and 3:1 is destination unreachable with a code of host unreachable. The list of ICMP types and codes can be found here http://www.iana.org/assignments/icmp-parameters/icmp-parameters.xml.
- **ip-protocol**
  Specifies the IP protocol against which the packet will be compared.
- **irule**
  Specifies the name of the iRule that will be triggered when a packet matches this firewall rule. The firewall rule match raises a FLOW_INIT iRule event.

- **irule-sample-rate**
  Specifies the rate at which an iRule specified by **irule** option will be triggered when a packet matches this firewall rule. The rate is an integer value in the range 0-65535 and specifies how many packets must match this firewall rule before the iRule is triggered. The default value is 1 and causes the iRule to be triggered for every packet that matches this firewall rule. A value of 0 disables iRule triggering.
- **log**
  Specifies whether the packet will be logged if it matches the rule. Logging must also be enabled using the **security-log-profiles** setting. Note that the statistics counter is always incremented when a packet matches a rule.
- **place-after**
  Specifies that a new rule should be placed after another rule, **first** or **last**. If individual rules are being added (as opposed to specifying **replace-all-with**) then **place-before** or **place-after** must be specified.
- **place-before**
  Specifies that a new rule should be placed before another rule, **first** or **last**. If individual rules are being added (as opposed to specifying **replace-all-with**) then **place-before** or **place-after** must be specified.
- **rule-list**
  Specifies a list of rules to evaluate. See **security firewall rule-list**. If a **rule-list** is specified then only the **schedule** and **status** properties effect the rule.
- **schedule**
  Specifies a schedule for the rule. See **security firewall schedule**. If the rule refers to a **rule-list** the **rule-list** will be enabled according to the schedule. When the **rule list** is enabled, the schedules defined within the **rule-list** will be honored.
- **source**

  - **address-lists**
    Specifies a list of address lists (see **security firewall address-list**) against which the packet will be compared.
  - **addresses**
    Specifies a list of addresses and networks against which the packet will be compared.
    The format for "ipv4" is *a*. *b*. *c*. *d* [*/ prefixlen*]. The format for an "ipv6" address is *a*: *b*: *c*: *d*: *e*: *f*: *g*: *h* [*/ prefixlen*].
  - **port-lists**
    Specifies a list of port lists (see **security firewall port-list**) against which the packet will be compared.
  - **ports**
    Specifies a list of ports and port ranges against which the packet will be compared.
  - **vlans**
    Specifies a list of vlans, vlan groups and tunnels against which the packet will be compared.

- **status**
  Specifies whether the rule is **enabled**, **disabled** or **scheduled**. A rule that is **enabled** is always checked. A rule that is **disabled** is never checked. A rule that is **scheduled** is checked according to the corresponding schedule configuration. A rule that is **scheduled** must have an associated schedule configuration.

- **fw-staged-policy**
  Specifies a staged firewall policy. **fw-staged-policy** rules are not enforced while all the visibility aspects namely statistics, reporting and logging function as if the **fw-staged-policy** rules were enforced on a virtual server.
- **fw-staged-policy-rules**
  Specifies firewall rules staged on **ltm virtual** via referenced **fw-staged-policy**.
- **glob**
  Displays the items that match the **glob** expression. See **help glob** for a description of **glob** expression syntax.
- **gtm-score**
  Specifies a score that is associated with the virtual server. Global Traffic Manager (GTM) can rely on this value to load balance traffic in a proportional manner.
- **http-class**
  Specifies a list of HTTP class profiles, separated by spaces, with which the virtual server works to increase the speed at which the virtual server processes HTTP requests. The default value is **none**. The order in which the profiles are entered sets the priority of each profile, in ascending order, specific to this virtual server.
- **ip-forward**
  Specifies a virtual server that has no pool members to load balance, but instead, forwards the packet directly to the destination IP address specified in the client request. If you specify the **ip-forward** option, you cannot use the **l2-forward** or **reject** options.
- **ip-protocol**
  Specifies the IP protocol for which you want the virtual server to direct traffic. Sample protocol names are TCP and UDP. The default value is **any**.

◆ Note

You do not use this setting when creating an HTTP class virtual server.

- **internal**
  Specifies an internal virtual server that handles requests for a parent virtual server, such as content adaptation. Internal virtual servers do not receive external connections, instead they are specified by name by profiles in the parent virtual server (see **ltm profile request-adapt** and **ltm profile response-adapt**). Since internal virtual servers do not listen for external connections, not all attributes are used for internal virtual

servers. The **destination**, **mask**, **translate-address**, **translate-port**, **vlans**, **vlans-disabled** and **vlans-enabled** attributes are set by the system, any attempt to change them will have no effect.

- **l2-forward**
  Specifies a virtual server that shares the same IP address as a node in an associated VLAN. You create this type of virtual server when you want to create a VLAN group. If you specify the **l2-forward** option, you cannot use the **ip-forward** or **reject** options.
- **last-hop-pool**
  Specifies the name of the last hop pool that you want the virtual server to use to direct reply traffic to the last hop router. The default value is **none**.
- **mask**
  Specifies the netmask for a network virtual server only. This setting is required for a network virtual server.
  The netmask clarifies whether the host bit is an actual zero or a wildcard representation. The default value is **255.255.255.255** for IPv4 or **ffff:ffff:ffff:ffff:ffff:ffff:ffff:ffff** for IPv6.
- **mirror**
  Enables or disables mirroring. You can use mirroring to maintain the same state information in the standby unit that is in the active unit, allowing transactions such as FTP file transfers to continue as though uninterrupted. The default value is **none**.
- **name**
  Specifies a unique name for the component. This option is required for the commands **create**, **delete**, and **modify**.
- **nat64**
  Enable or disable NAT64. The default value is **disabled**. NAT64 is a service that automatically translate IPv6 traffic into IPv4.
- **partition**
  Displays the name of the administrative partition within which the virtual server resides.
- **persist**
  Specifies a list of profiles separated by spaces that the virtual server uses to manage connection persistence. The default value is **none**.
  To enable persistence, typically you specify a single profile. However, you can specify multiple profiles in conjunction with iRules® that define a persistence strategy based on incoming traffic. In the case of multiple profiles, the **default** option specifies which profile you want the virtual server to use if an iRule does not specify a persistence method. When you specify multiple profiles, the default value of the default property is **no**. You can set the value of the **default** property to **yes** for only one of the profiles.
- **pool**
  Specifies a default pool to which you want the virtual server to automatically direct traffic. The default value is **none**.
- **profiles**
  Specifies a list of profiles for the virtual server to use to direct and manage traffic. The default value is **fastL4**.

- **rate-class**
  Specifies the name of an existing rate class that you want the virtual server to use to enforce a throughput policy for incoming network traffic. The default value is **none**.
- **rate-limit**
  Specifies the maximum number of connections per second allowed for a virtual server. The default value is ‘disabled’.
- **rate-limit-mode**
  Indicates whether the rate limit is applied per virtual object, per source address, per destination address, or some combination thereof. The default value is ‘object’, which does not use the source or destination address as part of the key.
- **rate-limit-dst-mask**
  Specifies a mask, in bits, to be applied to the destination address as part of the rate limiting. The default value is ‘0’, which is equivalent to using the entire address - ‘32’ in IPv4, or ‘128’ in IPv6.
- **rate-limit-src-mask**
  Specifies a mask, in bits, to be applied to the source address as part of the rate limiting. The default value is ‘0’, which is equivalent to using the entire address - ‘32’ in IPv4, or ‘128’ in IPv6.
- **regex**
  Displays the items that match the regular expression. The regular expression must be preceded by an at sign (@[regular expression]) to indicate that the identifier is a regular expression. See **help regex** for a description of regular expression syntax.
- **related-rules**
  Specifies a list of iRules, separated by spaces, that customize the behavior of secondary channels (for instance the data channel on FTP) opened on behalf of the virtual server. The default value is **none**.
- **reject**
  Specifies that the BIG-IP® system rejects any traffic destined for the virtual server IP address. If you specify the **reject** option, you cannot use the **ip-forward** or **l2-forward** options.
- **rules**
  Specifies a list of iRules, separated by spaces, that customize the virtual server to direct and manage traffic. The default value is **none**.
- **snat**
  Specifies whether SNAT automap is enabled for the virtual server. The default value is **none**. This attribute is DEPRECATED. Use **source-address-translation { type (automap / none) }**
- **snatpool**
  Specifies the name of an existing SNAT pool that you want the virtual server to use to implement selective and intelligent SNATs. This attribute is DEPRECATED. Use **source-address-translation { type snatpool pool** *pool_name* **}**

- **source**
  Specifies an IP address or network from which the virtual server will accept traffic.
  The format for an "ipv4" address is *a*. *b*. *c*. *d* [/ *prefixlen*]. The format for an "ipv6" address is *a*: *b*: *c*: *d*: *e*: *f*: *g*: *h* [/ *prefixlen*].
- **source-address-translation**
  Specifies the type of source address translation enabled for the virtual server as well as the pool that the source address translation will use.
  - **pool**
    Specifies the name of a LSN or SNAT pool used by the specified virtual server.
  - **type**
    Specifies the type of source address translation associated with the specified virtual server.
    The options are:
    - **automap**
      Specifies the use of self IP addresses for virtual server source address translation.
    - **lsn**
      Specifies the use of a LSN pool of translation addresses for virtual server source address translation.
    - **none**
      Specifies no source address translation to be used by the virtual server.
    - **snat**
      Specifies the use of a SNAT pool of translation addresses for virtual server source address translation.
- **source-port**
  Specifies whether the system preserves the source port of the connection. The default value is **preserve**.
  The options are:
  - **change**
    Obfuscates internal network addresses.
  - **preserve**
    Preserves the source port of the connection.
  - **preserve-strict**
    Use this value only for UDP under very special circumstances, such as nPath or transparent (that is, no translation of any other L3/L4 field), where there is a 1:1 relationship between virtual IP addresses and node addresses, or when clustered multi-processing (CMP) is disabled.
- **traffic-classes**
  Specifies a list of traffic classes that are associated with the virtual server. The default value is **none**.
- **translate-address**
  Enables or disables address translation for the virtual server. Disable address translation for a virtual server if you want to use the virtual

server to load balance connections to any address. This option is useful when the system is load balancing devices that have the same IP address. The default value is **disabled**.

- **translate-port**
  Enables or disables port translation. Disable port translation for a virtual server, if you want to use the virtual server to load balance connections to any service. The default value is **disabled**.
- **vlans**
  Specifies a list of VLANs on which the virtual server is either enabled or disabled. The default value is **none**. The options **vlans-disabled** and **vlans-enabled** indicate whether the virtual server is disabled or enabled on the list of specified VLANs.
- **vlans-disabled**
  Disables the virtual server on the VLANs specified in the **vlans** option. This is the default setting.
- **vlans-enabled**
  Enables the virtual server on the VLANs specified in the **vlans** option.
- **vs-index**
  Displays a unique index assigned to this virtual server.
- **metadata**
  Associates user defined data, each of which has name and value pair and persistence. Persistent(default) means the data will be saved into config file.
- **ip-intelligence-categories**
  Used to show/ reset statistics on IP intelligence white/ black lists categories.

See Also

create, *delete*, *edit*, glob, *list*, *ltm persistence*, *pool*, *modify*, *mv*, *vlan*, *vlan-group*, *schedule*, *rule-list*, regex, *reset-stats*, *rule*, *show*, *tmsh*

virtual-address

Configures virtual addresses.

Syntax

Configure the **virtual-address** component within the ltm module using the syntax shown in the following sections.

Create/Modify

```
create virtual address [name]
modify virtual address [name]
    address [ip address]
    app-service [[string] | none]
    arp [enabled | disabled]
    auto-delete [true | false]
    connection-limit [integer]
    description [string]
    enabled [yes | no]
    icmp-echo [enabled | disabled]
    mask [netmask]
    route-advertisement [enabled | disabled]
    server-scope [all | any | none]
    traffic-group [[string] | default | non-default | none]
    metadata
      [add | delete | modify] {
        [metadata_name ... ] {
          value [ "value content" ]
          persist [ true | false ]
        }
    }
edit virtual-address [ [ [name] | [glob] | [regex] ] ... ]
     all-properties
    non-default-properties
reset-stats virtual-address
reset-stats virtual-address [ [ [name] | [glob] | [regex] ] ... ]
mv virtual-address [ [[source-name] [destination-name]] | [[name] to-folder
[folder-name]] | [[name...name] to-folder [folder-name]] ]
    to-folder
```

Display

```
list virtual-address
list virtual-address [ [ [name] | [glob] | [regex] ] ... ]
show running-config virtual-address
show running-config virtual-address
                    [ [ [name] | [glob] | [regex] ] ... ]
    all-properties
    non-default-properties
    one-line
    partition
show virtual-address
show virtual-address [ [ [name] | [glob] | [regex] ] ... ]
   all-properties
```

```
(default | exa | gig | kil | meg | peta | raw | tera | yotta | zetta)
detail
field-fmt
```

Delete

```
delete virtual-address [all | [name]]
```

Description

You can use the **virtual-address** component to enable, disable, display, and delete virtual addresses. You can also list the virtual address configuration, and view statistics for a specific virtual address.

Note that **tmsh** only displays virtual addresses when you explicitly request them. For example:

To display the properties of virtual addresses or a specific virtual address from the **ltm** module, use the command sequences **list virtual-address** and **list virtual-address [name]**, respectively.

To display statistics for virtual addresses or a specific virtual address from the **ltm** module, use the command sequence **show virtual-address** and **show virtual-address [name]**, respectively.

Examples

create virtual-address myVirtualAddr address 10.10.10.20 enabled yes

Creates a virtual address 10.10.10.20, with a name of myVirtualAddr.

create virtual-address myVirtualAddr address 10.10.10.20 enabled yes traffic-group /Common/traffic-group-1

Creates a virtual address 10.10.10.20, with a name of myVirtualAddr, that is assigned to traffic-group-1.

modify virtual-address myVirtualAddr enabled no

Disables the virtual address myVirtualAddr.

delete virtual-address myVirtualAddr

Deletes the virtual address myVirtualAddr.

list virtual-address myVirtualAddr all-properties

Lists the configuration information for the virtual address, myVirtualAddr.

show virtual-address myVirtualAddr

Displays statistics and status for the virtual-address **myVirtualAddr**.

show virtual-address myVirtualAddr all-properties

Displays statistics and status for the virtual named **myVirtualAddr**.

Note that if the system includes Packet Velocity® ASIC (PVA) and PVA Assist capabilities, this command displays status and statistics for that feature.

mv /ltm virtual-address /Common/10.10.10.20 to-folder /Common/all_virtual_addresses

Moves the virtual-address **10.10.10.20** to a folder named **all_virtual_addresses**.

◆ Note

If you wish to change the name of the virtual-address, you must use the configured IP Address or a name that does not represent a different IP Address than the one configured.

Please refer to the **mv** manual page for additional examples on how to use the mv command.

Options

- **address**
  The virtual IP address.
- **arp**
  Enables or disables ARP for the specified virtual address. The default value is **enabled**.
- **app-service**
  Specifies the name of the application service to which the virtual address belongs. The default value is **none**. **Note:** If the **strict-updates** option is **enabled** on the application service that owns the object, you cannot modify or delete the virtual address. Only the application service can modify or delete the virtual address.
- **auto-delete**
  Indicates if the virtual address will be deleted automatically on deletion of the last associated virtual server or not. The default value is **true**.
- **connection-limit**
  Sets a concurrent connection limit for one or more virtual servers. The default value is **0**, meaning "no limit."
- **description**
  User defined description.
- **enabled**
  Specifies whether the specified virtual address is enabled. The default value is **yes**.
- **floating**
  Read-only property derived from **traffic-group**. A floating virtual address is a virtual address for a VLAN that serves as a shared address by all devices of a BIG-IP traffic-group.
- **glob**
  Displays the items that match the **glob** expression. See **help glob** for a description of **glob** expression syntax.

- **icmp-echo**
  Enables or disables ICMP echo replies for the specified virtual address. The default value is **enabled**.
- **mask**
  Sets the netmask for one or more network virtual servers only. This setting is required for network virtual servers. The default value is **255.255.255.255**.
- **partition**
  Displays the administrative partition within which the virtual address resides.
- **regex**
  Displays the items that match the regular expression. The regular expression must be preceded by an at sign (@[regular expression]) to indicate that the identifier is a regular expression. See **help regex** for a description of regular expression syntax.
- **route advertisement**
  Enables or disables route advertisement for the specified virtual address. The default value is **disabled**.
- **server-scope**
  Specifies the server that uses the specified virtual address. The default value is **any**.
- **unit**
  Read-only property that specifies the unit in a redundant system. Based on **traffic-group**.
- **traffic-group**
  Specifies the traffic group on which the virtual address is active. The default traffic group is inherited from the containing folder.
- **inherited-traffic-group**
  Read-only property that indicates if the **traffic-group** is inherited from the parent folder.
- **metadata**
  Associates user defined data, each of which has name and value pair and persistence. Persistent(default) means the data will be saved into config file.

See Also

create, *delete*, *edit*, glob, *list*, *virtual*, *modify*, *mv*, regex, *reset-stats*, *show*, *tmsh*

50

ltm auth

- Introducing the ltm auth module
- Alphabetical list of components

Introducing the ltm auth module

You can use the tmsh components that reside within the ltm auth module to configure profiles for Local Traffic Manager™. For more information about the tmsh hierarchical structure, see Chapter 2, *Understanding and Using the Traffic Management Shell*.

Alphabetical list of components

The remainder of this chapter lists the tmsh components that are available in the ltm auth module.

crldp-server

Creates a Certificate Revocation List Distribution Point (CRDLP) server for implementing a CRLDP authentication module.

Syntax

Configure the **crldp-server** component within the **ltm auth** module using the syntax in the following sections.

Create/Modify

```
create crldp-server [name]
modify crldp-server [name]
    app-service [[string] | none]
    base-dn [ [LDAP base directory name] | none]
    description [string]
    host [ [ip address] | none]
    port [ [name] | [number] ]
    reverse-dn [disabled | enabled]
edit crldp-server [ [ [name] | [glob] | [regex] ] ... ]
    all-properties
    non-default-properties
```

Display

```
list crldp-server
list crldp-server [ [ [name] | [glob] | [regex] ] ... ]
show running-config crldp-server
show running-config crldp-server [ [ [name] | [glob] | [regex] ] ... ]
    all-properties
    non-default-properties
    one-line
    partition
```

Delete

```
delete crldp-server [name]
```

Description

CRLDP authentication is a mechanism for checking certificate revocation status for client connections passing through the BIG-IP® system. This module is useful when your authentication data is stored on a remote CRLDP server.

To implement a CRLDP authentication module and create a CRLDP server:

1. Use the **crldp-server** component in the **ltm auth** module to create a CRLDP server.

2. Use the **ssl-crldp** component in the **ltm auth** module to configure a CRLDP configuration object and associate it with the server you created in Step 1.

3. Use the **profile** component in the **ltm auth** module to create an authentication profile in which you specify the following options:

   a) For the **configuration** option, specify the SSL CRLDP configuration object that you created in Step 2.

   b) For the **defaults-from** option, specify a parent profile (either the default profile named **ssl_crldp** or another custom profile that you created).

Examples

create crldp-server my_crldp_server

Creates a CRLDP server named my_crldp_server.

delete crldp-server my_crldp_server

Deletes a CRLDP server named my_crldp_server.

Options

- **app-service**
  Specifies the name of the application service to which the CRLDP server belongs. The default value is **none**. **Note:** If the **strict-updates** option is **enabled** on the application service that owns the object, you cannot modify or delete the CRLDP server. Only the application service can modify or delete the CRLDP server.
- **base-dn**
  Specifies the LDAP base directory name for certificates that specify the CRL distribution point in directory name format (dirName). The default value is **none**.
  Use this option when the value of the X509v3 attribute **crlDistributionPoints** is of type **dirName**. In this case, the BIG-IP system attempts to match the value of the **crlDistributionPoints** attribute to the value of the **base-dn** option. An example of a **base-dn** value is **cn=lxxx,dc=f5,dc=com**.
- **description**
  User defined description.
- **glob**
  Displays the items that match the **glob** expression. See **help glob** for a description of **glob** expression syntax.

- **host**
  Specifies an IP address for the CRLDP server. This option is required. The default value is **none**.
- **name**
  Specifies a unique name for the component. This option is required for the commands **create**, **delete**, and **modify**.
- **partition**
  Displays the administrative partition within which the component resides.
- **port**
  Specifies the port for CRLDP authentication traffic. The default value is **389**.
- **regex**
  Displays the items that match the regular expression. The regular expression must be preceded by an at sign (@[regular expression]) to indicate that the identifier is a regular expression. See **help regex** for a description of regular expression syntax.
- **reverse-dn**
  Specifies in which order the system attempts to match the value of the **base-dn** option to the value of the X509v3 attribute **crlDistributionPoints**. When **enabled**, the system matches the value of the **base-dn** option from left to right, or from the beginning of the DN string, to accommodate dirName strings in certificates such as **C=US,ST=WA,L=SEA,OU=F5,CN=xxx**. The default value is **disabled**.

See Also

create, *delete*, *edit*, glob, *list*, *profile*, *ssl-crldp*, *virtual*, *modify*, *reset-stats*, regex, *reset-stats*, *show*, *tmsh*

kerberos-delegation

Configures a Kerberos delegation profile.

Syntax

Configure the **kerberos-delegation** component within the **ltm auth** module using the syntax shown in the following sections.

Create/Modify

```
create kerberos-delegation [name]
modify kerberos-delegation [name]
    app-service [[string] | none]
    client-principal [string]
    debug-logging [disabled | enabled]
    description [string]
    protocol-transition [disabled | enabled]
    server-principal [string]

edit kerberos-delegation [ [ [name] | [glob] | [regex] ] ... ]
    all-properties
    non-default-properties

reset-stats kerberos-delegation
reset-stats kerberos-delegation
  [ [ [name] | [glob] | [regex] ] ... ]
```

Display

```
list kerberos-delegation
list kerberos-delegation [ [ [name] | [glob] | [regex] ] ... ]
show running-config kerberos-delegation
show running-config kerberos-delegation
  [ [ [name] | [glob] | [regex] ] ... ]
    all-properties
    non-default-properties
    one-line
    partition

show kerberos-delegation
show kerberos-delegation [ [ [name] | [glob] | [regex] ] ... ]
    (default | exa | gig | kil | meg | peta | raw | tera | yotta | zetta)
    field-fmt
    global
```

Delete

```
delete kerberos-delegation [name]
```

Description

The Kerberos delegation configuration acts like a proxy for Kerberos credentials. When connecting to a server that is inside its domain, the browser client fetches Kerberos credentials known as delegated credentials.

These credentials are passed on to the system. Once the system has these credentials, it retrieves credentials for the RealServer® that is on the back end, and passes those credentials back.

Each user is assigned a unique cookie that describes a session on the system. This cookie is encrypted in a cookie key.

To configure a Kerberos authentication module and create a Kerberos configuration object:

1. Use the kerberos-delegation component in the **ltm auth** module to create a Kerberos configuration object.

2. Use the profile component, in the **ltm auth** module, to create an authentication profile in which you specify the following options:

   a) For the configuration option, specify the Kerberos configuration object that you created in Step 1.

   b) For the defaults-from option, specify a parent profile (either the default Kerberos profile named krbdelegate or another custom Kerberos profile that you created).

Examples

create kerberos-delegation my_kerberos-delegation_config client-principal client.net server-principal server.net

Creates a Kerberos delegation profile named **my_kerberos-delegation_config**.

list kerberos-delegation all-properties

Displays all properties for all Kerberos delegation profiles.

Options

- **app-service**
  Specifies the name of the application service to which the profile belongs. The default value is **none**. **Note:** If the **strict-updates** option is **enabled** on the application service that owns the object, you cannot modify or delete the profile. Only the application service can modify or delete the profile.
- **client-principal**
  Specifies the principal that the client sees. This is usually a value such as HTTP/<fqdn>. This principal may be in a different domain from the server principal. This option is required. There is no default value.
- **debug-logging**
  Specifies whether the system logs debugging actions. The default value is **disabled**.

- **description**
  User defined description.
- **glob**
  Displays the items that match the **glob** expression. See **help glob** for a description of **glob** expression syntax.
- **name**
  Specifies a unique name for the component. This option is required for the commands **create**, **delete**, and **modify**.
- **partition**
  Displays the administrative partition within which this profile resides.
- **protocol-transition**
  Specifies whether associated virtual should transition client certificate authentication into Kerberos credentials.
- **regex**
  Displays the items that match the regular expression. The regular expression must be preceded by an at sign (@[regular expression]) to indicate that the identifier is a regular expression. See **help regex** for a description of regular expression syntax.
- **server-principal**
  Specifies the principal of the back-end web server. This is usually a value such as HTTP/<fqdn of server>. This may be in a different domain from the server principal. This setting is required. There is no default value.

See Also

create, *delete*, *edit*, glob, *list*, *virtual*, *modify*, regex, *reset-stats*, *show*, *tmsh*

ldap

Configures an LDAP configuration object for implementing remote LDAP-based client authentication.

Syntax

Configure the **ldap** component within the **ltm auth** module using the syntax shown in the following sections.

Create/Modify

```
create ldap [name]
modify ldap [name]
    bind-dn [ [account dn] | none]
    bind-pw [ [string] | none]
    bind-timeout [integer]
    check-host-attr [disabled | enabled]
    debug [disabled | enabled]
    description [string]
    filter [ [string] | none]
    group-dn [ [group dn] | none]
    group-member-attr [ [string] | none]
    idle-timeout [integer]
    ignore-auth-info-unavail [no | yes]
    ignore-unknown-user [disabled | enabled]
    login-attribute [ [account name] | none]
    port [ [name] | [integer]]
    scope [base | one | sub]
    search-base-dn [ [search base dn] | none]
    search-timeout [number]
    servers
      [add | delete | replace-all-with] {
        [ip address ... ]
    }
    servers none
    ssl [disabled | enabled]
    ssl-ca-cert-file [ [name] | none)
    ssl-check-peer [disabled | enabled]
    ssl-ciphers [ [string] | none]
    ssl-client-cert [ [string] | none]
    ssl-client-key [ [string] | none]
    user-template [ [string] | none]
    version [number]
    warnings [disabled | enabled]
edit ldap [ [ [name] | [glob] | [regex] ] ... ]
   all-properties
   non-default-properties
```

Display

```
list ldap
list ldap [ [ [name] | [glob] | [regex] ] ... ]
show running-config ldap
show running-config ldap [ [ [name] | [glob] | [regex] ] ... ]
    all-properties
```

```
non-default-properties
one-line
partition
```

Delete

```
delete ldap [name]
```

Description

LDAP authentication is a mechanism for authenticating or authorizing client connections passing through the system. LDAP authentication is useful when your authentication or authorization data is stored on a remote LDAP server or a Microsoft® Windows Active Directory® server, and you want the client credentials to be based on basic HTTP authentication (that is, user name and password).

To configure an LDAP authentication module and create an LDAP configuration object:

1. Use the **ldap** component in the **ltm auth** module to create an LDAP configuration object.

2. Use the **profile** component, in the **ltm auth** module, to create an authentication profile in which you specify the following options:

   a) For the **configuration** option, specify the LDAP configuration object that you created in Step 1.

   b) For the **defaults-from** option, specify a parent profile (either the default LDAP profile named **ldap** or another custom profile that you created).

Examples

create ldap my_auth_ldap servers add {my_ldap_auth_server}

Creates a configuration object named **my_auth_ldap**

delete ldap my_auth_ldap

Deletes the configuration object named **my_auth_ldap**.

Options

- **bind-dn**
  Specifies the distinguished name of an account to which to bind, to perform searches. This search account is a Read-only account used to do searches. You can use the **admin** account as the search account. If no

admin DN is specified, then no bind is attempted. The default value is **none**.
This option is required only when a site does not allow anonymous searches. If the remote server is a Microsoft® Windows® Active Directory® server, the distinguished name must be in the form of an email address.

- **bind-pw**
Specifies the password for the search account created on the LDAP server. This option is required if you specify a value for the **bind-dn** option. The default value is **none**.
- **bind-timeout**
Specifies a bind timeout limit. The default value is **30** seconds.
- **check-host-attr**
Confirms the password for the bind distinguished name. This option is optional. The default value is **disabled**.
- **debug**
Enables or disables syslog-ng debugging information at LOG DEBUG level. The default value is **disabled**. F5 Networks does not recommend using this option for normal configuration.
- **description**
User defined description.
- **filter**
Specifies a filter. Use this option for authorizing client traffic. The default value is **none**.
- **glob**
Displays the items that match the **glob** expression. See **help glob** for a description of **glob** expression syntax.
- **group-dn**
Specifies the group distinguished name. The system uses this option for authorizing client traffic. The default value is **none**.
- **group-member-attribute**
Specifies a group member attribute. The system uses this option for authorizing client traffic. The default value is **none**.
- **idle-timeout**
Specifies the idle timeout, in seconds, for connections. The default value is **3600** seconds.
- **ignore-auth-info-unavail**
Specifies whether the system ignores authentication information, if it is not available. The default value is **no**.
- **ignore-unknown-user**
Specifies whether the system ignores a user that is unknown. The default value is **disabled**.
- **login-attribute**
Specifies a logon attribute. Normally, the value for this option is **uid**; however, if the server is a Microsoft Windows Active Directory server, the value must be the account name **samaccountname** (not case-sensitive). The default value is **none**.

- **name**
  Specifies a unique name for the component. This option is required for the commands **create**, **delete**, and **modify**.
- **partition**
  Displays the administrative partition within which the component resides.
- **port**
  Specifies the port number or name for the LDAP service. Port **389** is typically used for non-SSL and port **636** is used for an SSL-enabled LDAP service. The default value is **ldap**.
- **regex**
  Displays the items that match the regular expression. The regular expression must be preceded by an at sign (@[regular expression]) to indicate that the identifier is a regular expression. See **help regex** for a description of regular expression syntax.
- **scope**
  Specifies the search scope. The default value is **sub**. The options are:
  - **base**
    Specifies the search scope is base object. The **base** value is almost never useful for nameservice lookups.
  - **one**
    Specifies the search scope is one level.
  - **sub**
    Specifies the search scope is subtree.
- **search-base-dn**
  Specifies the search base distinguished name. The default value is **none**.
- **search-timeout**
  Specifies the search timeout. The default value is **30** seconds.
- **servers**
  Specifies the LDAP servers that the system must use to obtain authentication information. You must specify a server when you create an LDAP configuration object.
- **ssl**
  Enables or disables SSL functionality. The default is **disabled**.
  Note that when you use the command line interface to enable SSL for an LDAP service, the system does not change the service port number from 389 to 636, as is required. To change the port number from the command line, use the **service** option of this command (see above), for example, **ldap [name] ssl enabled service 636**.
- **ssl-ca-cert-file**
  Specifies the name of an SSL CA certificate using the full path to the file. The default value is **none**.
- **ssl-check-peer**
  Specifies whether the system checks an SSL peer. The default value is **disabled**.
- **ssl-ciphers**
  Specifies SSL ciphers. The default value is **none**.

- **ssl-client-cert**
  Specifies the name of an SSL client certificate. The default value is **none**.
- **ssl-client-key**
  Specifies the name of an SSL client key. The default value is **none**.
- **user-template**
  Specifies a user template for the LDAP application to use for authentication. The default value is **none**.
- **version**
  Specifies the version number of the LDAP application. The default value is **3**.
- **warnings**
  Enables or disables warning messages. The default value is **enabled**.

See Also

create, *delete*, *edit*, glob, *list*, *profile*, *virtual*, *modify*, regex, *reset-stats*, *show*, *tmsh*

ocsp-responder

Configures Online Certificate System Protocol (OCSP) responder objects.

Syntax

Configure the **ocsp-responder** component within the **ltm auth** module using the syntax shown in the following sections.

Create/Modify

```
create ocsp-responder [name]
modify ocsp-responder [name]
    allow-certs [disabled | enabled]
    app-service [[string] | none]
    ca-file [ [file name] | none]
    ca-path [ [file name] | none]
    cert-id-digest [md5 | sha1]
    chain [disabled | enabled]
    check-certs [disabled | enabled]
    description [string]
    explicit [disabled | enabled]
    ignore-aia [disabled | enabled]
    intern [disabled | enabled]
    nonce [disabled | enabled]
    sign-digest [md5 | sha1]
    sign-key [ [key] | none)
    sign-key-pass-phrase [ [pass phrase] | none]
    sign-other [ [list of certs] | none]
    signer [ [certificate] | none]
    status-age [integer]
    trust-other [disabled | enabled]
    url [none | [url] ]
    va-file [ [file name] | none]
    validity-period [integer]
    verify [disabled | enabled]
    verify-cert [disabled | enabled]
    verify-other [ [file name] | none]
    verify-sig [disabled | enabled]
edit ocsp-responder [ [ [name] | [glob] | [regex] ] ... ]
    all-properties
    non-default-properties
```

Display

```
list ocsp-responder
list ocsp-responder [ [ [name] | [glob] | [regex] ] ... ]
show running-config ocsp-responder
show running-config ocsp-responder [ [ [name] | [glob] | [regex] ] ... ]
    all-properties
    non-default-properties
    one-line
    partition
```

Delete

```
delete ocsp-responder [name]
```

Description

To implement the SSL OCSP authentication module, you must create the following objects: one or more OCSP responder objects, an SSL OCSP configuration object, and an SSL OCSP profile.

To implement an SSL OCSP authentication module and create an OCSP responder object:

1. Use the **ocsp-responder** component in the **ltm auth** module to configure an OCSP responder object.

2. Use the **ssl-ocsp** component in the **ltm auth** module to configure an SSL OCSP configuration object to which you add the OCSP responder object that you created in Step 1.

3. Use the **profile** component in the **ltm auth** module to create an authentication profile in which you specify the following options:

   a) For the **configuration** option, specify the SSL OCSP configuration object that you created in Step 2.

   b) For the **defaults-from** option, specify a parent profile (either the default OCSP Responder profile named **ssl_ocsp** or another custom profile that you created).

Options

- **allow-certs**
  Enables or disables the addition of certificates to an OCSP request. The default value is **enabled**.
- **app-service**
  Specifies the name of the application service to which the OCSP responder object belongs. The default value is **none**. **Note:** If the **strict-updates** option is **enabled** on the application service that owns the object, you cannot modify or delete the OCSP responder object. Only the application service can modify or delete the OCSP responder object.
- **ca-file**
  Specifies the name of the file containing trusted CA certificates used to verify the signature on the OCSP response. The default value is **none**.

- **ca-path**
  Specifies the name of the path containing trusted CA certificates used to verify the signature on the OCSP response. The default value is **none**.
- **cert-id-digest**
  Specifies a specific algorithm identifier, either **sha1** or **md5**. The default value is **sha1**. The options are:
  - **sha1** is newer and provides more security with a 160-bit hash length.
  - **md5** is older and has only a 128-bit hash length.

The cert ID is part of the OCSP protocol. The OCSP client (in this case, the BIG-IP system) calculates the cert ID using a hash of the Issuer and serial number for the certificate that it is trying to verify.

- **chain**
  Specifies whether the system constructs a chain from certificates in the OCSP response. The default value is **enabled**.
- **check-certs**
  Enables or disables verification of an OCSP response certificate. Use this option for debugging purposes only. The default value is **enabled**.
- **description**
  User defined description.
- **explicit**
  Specifies that the Local Traffic Manager explicitly trusts that the OCSP response signer's certificate is authorized for OCSP response signing. If the signer's certificate does not contain the OCSP signing extension, specification of this option causes a response to be untrusted. The default value is **enabled**.
- **glob**
  Displays the items that match the **glob** expression. See **help glob** for a description of **glob** expression syntax.
- **ignore-aia**
  Specifies whether the system ignores the URL contained in the certificate's AIA fields, and always uses the URL specified by the responder instead. The default value is **disabled**.
- **intern**
  Specifies whether the system ignores certificates contained in an OCSP response when searching for the signer's certificate. To use this option, the signer's certificate must be specified with either the **verify-other** or **va-file** option. The default value is **enabled**.
- **name**
  Specifies a unique name for the component. This option is required for the commands **create**, **delete**, and **modify**.
- **nonce**
  Specifies whether the system verifies an OCSP response signature or the nonce values. The default value is **enabled**.

- **partition**
  Displays the administrative partition within which the component resides.
- **regex**
  Displays the items that match the regular expression. The regular expression must be preceded by an at sign (@[regular expression]) to indicate that the identifier is a regular expression. See **help regex** for a description of regular expression syntax.
- **sign-digest**
  Specifies the algorithm for signing the request, using the signing certificate and key. This parameter has no meaning, if request signing is not in effect (that is, both the request signing certificate and request signing key parameters are empty). This parameter is required only when request signing is in effect. The default value is **sha1**.
- **sign-key**
  Specifies the key that the system uses to sign an OCSP request. The default value is **none**.
- **sign-key-pass-phrase**
  Specifies the passphrase that the system uses to encrypt the sign key. The default value is **none**.
- **sign-other**
  Adds a list of additional certificates to an OCSP request. The default value is **none**.
- **signer**
  Specifies a certificate used to sign an OCSP request. If the certificate is specified, but the key is not specified, then the private key is read from the same file as the certificate. If neither the certificate nor the key is specified, then the request is not signed. If the certificate is not specified and the key is specified, then the configuration is considered to be invalid. The default value is **none**.
- **status-age**
  Specifies the age of the status of the OCSP responder. The default value is **0** (zero).
- **trust-other**
  Instructs the BIG-IP local traffic management system to trust the certificates specified with the **verify-other** option. The default is value **disabled**.
- **url**
  Specifies the URL used to contact the OCSP service on the responder. This option is required. The default value is **none**.
- **va-file**
  Specifies the name of the file containing explicitly trusted responder certificates. This parameter is needed in the event that the responder is not covered by the certificates already loaded into the responder's CA store. The default value is **none**.

- **validity period**
  Specifies the number of seconds used to specify an acceptable error range. Use this option when the OCSP responder clock and a client clock are not synchronized, which can cause a certificate status check to fail. This value must be a positive number. The default value is **300** seconds.
- **verify**
  Enables or disables verification of an OCSP response signature or the nonce values. Used for debugging purposes only. The default value is **enabled**.
- **verify-cert**
  Specifies that the system makes additional checks to see if the signer's certificate is authorized to provide the necessary status information. Use this option for testing purposes only. The default value is **enabled**.
- **verify-other**
  Specifies the name of the file used to search for an OCSP response signing certificate when the certificate has been omitted from the response. The default value is **none**.
- **verify-sig**
  Specifies that the system checks the signature on the OCSP response. Use this option for testing purposes only. The default value is **enabled**.

See Also

create, *delete*, *edit*, glob, *list*, *profile*, *ssl-ocsp*, *virtual*, *modify*, regex, *show*, *tmsh*

profile

Configures an authentication profile.

Syntax

Configure the **profile** component within the **ltm auth** module using the syntax shown in the following sections.

Create/Modify

```
create profile [name]
modify profile [name]
    app-service [[string] | none]
    configuration [ [name] | none]
    cookie-key [string]
    cookie-name [string]
    credential-source [http-basic-auth]
    defaults-from [name]
    description [string]
    enabled [yes | no]
    idle-timeout [integer]
    rule [iRule name]
edit profile [ [ [name] | [glob] | [regex] ] ... ]
      all-properties
      non-default-properties
reset-stats profile
reset-stats profile [ [ [name] | [glob] | [regex] ] ... ]
```

Display

```
list profile
list profile [ [ [name] | [glob] | [regex] ] ... ]
show running-config profile
show running-config profile [ [ [name] | [glob] | [regex] ] ... ]
    all-properties
    non-default-properties
    one-line
    partition
show profile
show profile [ [ [name] | [glob] | [regex] ] ... ]
   (default | exa | gig | kil | meg | peta | raw | tera | yotta | zetta)
   field-fmt
   global
```

Delete

```
delete profile [name]
```

Note

You cannot delete default profiles.

Description

You can use the **profile** component to configure a custom authentication profile, or you can use the default profile that the BIG-IP® Local Traffic Manager system provides for each type of authentication module.

An authentication profile requires one of the following configuration objects: **ltm auth kerberos-delegation**, **ltm auth ldap**, **ltm auth radius**, **ltm auth ssl-cc-ldap**, **ltm auth ssl-crldp**, **ltm auth ssl-ocsp** or **ltm auth tacacs**. The type of profile specified by the **defaults-from** option must match the type of configuration object.

Examples

create profile my_authentication_profile { configuration tacacs defaults-from tacacs credential-source http-basic-auth enabled yes idle-timeout 30 rule _sys_auth_tacacs }

Creates a profile named **my_authentication_profile** for TACACS+ authentication.

list profile

Displays the properties of all of the auth profile components.

Options

- **app-service**
  Specifies the name of the application service to which the profile belongs. The default value is **none**. **Note:** If the **strict-updates** option is **enabled** on the application service that owns the object, you cannot modify or delete the profile. Only the application service can modify or delete the profile.
- **configuration**
  Specifies the name of an authentication configuration object. This option is required.
- **cookie-key**
  Specifies the key that the system uses to encrypt the session cookie assigned to each user using the **cookie-name** option. The default value is **f5auth**. This option applies only to KRB Delegate profiles.
- **cookie-name**
  Specifies a session cookie that the system assigns to each user. F5 Networks recommends that each virtual server use a different cookie name. The system encrypts the cookie using the value of the **cookie-key** option. The default value is **abc123**. This option applies only to KRB Delegate profiles.
- **credential-source**
  Specifies the credential source.

- **defaults-from**
  Specifies the name of the authentication profile from which you want your custom profile to inherit settings. This option is required.
- **description**
  User defined description.
- **enabled**
  Specifies whether this authentication profile is enabled. The default value is **yes**.
- **glob**
  Displays the items that match the **glob** expression. See **help glob** for a description of **glob** expression syntax.
- **idle-timeout**
  Specifies the idle timeout for the authentication profile. The default value is **300** seconds.
- **name**
  Specifies a unique name for the component. This option is required for the commands **create**, **delete**, and **modify**.
- **partition**
  Displays the administrative partition within which the component resides.
- **regex**
  Displays the items that match the regular expression. The regular expression must be preceded by an at sign (@[regular expression]) to indicate that the identifier is a regular expression. See **help regex** for a description of regular expression syntax.
- **rule**
  Specifies the name of the rule that corresponds to the authentication method you want to use.

See Also

create, *delete*, *edit*, glob, *crldp-server*, *kerberos-delegation*, *ldap*, *ocsp-responder*, *radius*, *radius-server*, *ssl-cc-ldap*, *ssl-crldp*, *ssl-ocsp*, *tacacs*, *list*, *virtual*, *modify*, regex, *reset-stats*, *show*, *tmsh*

radius

Configures a RADIUS configuration object for implementing remote RADIUS-based authentication of BIG-IP® system users.

Syntax

Configure the **radius** component within the **ltm auth** module using the syntax shown in the following sections.

Create/Modify

```
create radius [name]
modify radius [name]
    accounting-bug [disabled | enabled]
    client-id [none | [string]]
    debug [disabled | enabled]
    description [string]
    retries [integer]
    service-type [default | login | framed | callback-login | callback-framed |
outbound | administrative | nas-prompt | authenticate-only | callback-nas-prompt |
call-check | callback-administrative]
servers
  [add | delete | replace-all-with] {
    [ [hostname ... ] | [ip address ... ] ]
}
servers [default | none]
edit radius [ [ [name] | [glob] | [regex] ] ... ]
   all-properties
   non-default-properties
```

Display

```
list radius
list radius [ [ [name] | [glob] | [regex] ] ... ]
show running-config radius
show running-config radius [ [ [name] | [glob] | [regex] ] ... ]
    all-properties
    non-default-properties
    one-line
    partition
```

Delete

```
delete radius [name]
```

Description

You use a RADIUS authentication module when your authentication data is stored on a remote RADIUS server. In this case, client credentials are based on basic HTTP authentication (that is, username and password).

To implement a RADIUS authentication module and create a RADIUS configuration object:

1. Use the **radius-server** component in the **ltm auth** module to configure a RADIUS server.

2. Use the **radius** component in the **ltm auth** module to create a RADIUS configuration object that references the RADIUS server you created in Step 1.

3. Use the **profile** component in the **ltm auth** module to create an authentication profile in which you specify the following options:

   a) For the **configuration** option, specify the RADIUS configuration object that you created in Step 2.

   b) For the **defaults-from** option, specify a parent profile (either the default RADIUS profile named **radius** or another custom profile that you created).

Examples

create radius my_radius_auth servers add { myradiusserver }

Creates a RADIUS configuration object named **my_radius_auth**.

delete radius my_radius_auth

Deletes the RADIUS configuration object named **my_radius_auth**.

Options

- **accounting-bug**
  Enables or disables validation of the accounting response vector. This option is necessary only on older servers. The default value is **disabled**.
- **client-id**
  Sends a NAS-Identifier RADIUS attribute with string bar. If you do not specify a value for the **client-id** option, the system uses the pluggable authentication module (PAM) service type. You can disable this feature by specifying a blank client ID.
- **debug**
  Enables or disables syslog-ng debugging information at LOG DEBUG level. F5 Networks does not recommend this option for normal use. The default value is **disabled**.
- **description**
  User defined description.

- **glob**
  Displays the items that match the **glob** expression. See **help glob** for a description of **glob** expression syntax.
- **name**
  Specifies a unique name for the component. This option is required for the commands **create**, **delete**, and **modify**.
- **partition**
  Displays the administrative partition within which the component resides.
- **regex**
  Displays the items that match the regular expression. The regular expression must be preceded by an at sign (@[regular expression]) to indicate that the identifier is a regular expression. See **help regex** for a description of regular expression syntax.
- **retries**
  Specifies the number of authentication retries that the Local Traffic Manager allows before authentication fails. The default value is **3**.
- **service-type**
  Specifies the type of service used for the RADIUS server. The default is **default**, which behaves as **authenticate-only**.
- **servers**
  Specifies the hostnames or IP addresses of the RADIUS servers that the BIG-IP Local Traffic Manager uses to obtain authentication data.

See Also

create, *delete*, *edit*, glob, *list*, *profile*, *radius-server*, *virtual*, *modify*, regex, *show*, *tmsh*

radius-server

Configures a RADIUS server for implementing remote RADIUS-based client authentication.

Syntax

Configure the **radius-server** component within the **ltm auth** module using the syntax shown in the following sections.

Create/Modify

```
create radius-server [name]
modify radius-server [name]
    description [string]
    port [ [name] | [number]]
    secret [none | ["string"] ]
    server [ [hostname] | [ip address] | none ]
    timeout [integer]
edit radius-server [ [ [name] | [glob] | [regex] ] ... ]
    all-properties
    non-default-properties
```

Display

```
list radius-server
list radius-server [ [ [name] | [glob] | [regex] ] ... ]
show running-config radius-server
show running-config radius-server [ [ [name] | [glob] | [regex] ] ... ]
    all-properties
    non-default-properties
    one-line
    partition
```

Delete

```
delete radius-server [name]
```

Description

You use a RADIUS authentication module when your authentication data is stored on a remote RADIUS server. In this case, client credentials are based on basic HTTP authentication (that is, user name and password).

To configure a RADIUS authentication module and create a RADIUS server:

1. Use the **radius-server** component in the **ltm auth** module to configure a RADIUS server.

2. Use the **radius** component in the **ltm auth** module to create a RADIUS configuration object that references the RADIUS server you created in Step 1.

3. Use the **profile** component in the **ltm auth** module to create an authentication profile in which you specify the following options:

   a) For the **configuration** option, specify the **radius** component that you created in Step 2.

   b) For the **defaults-from** option, specify a parent profile (either the default RADIUS profile named **radius** or another custom profile that you created).

Examples

create radius-server bigip_auth_radius_server secret "This is the secret." server 10.1.1.1

Creates a RADIUS server named **my_radius_server**.

delete radius-server my_radius_server

Deletes the RADIUS server named **my_radius_server**.

Options

- **description**
  User defined description.
- **glob**
  Displays the items that match the **glob** expression. See **help glob** for a description of **glob** expression syntax.
- **name**
  Specifies a unique name for the component. This option is required for the commands **create**, **delete**, and **modify**.
- **partition**
  Displays the administrative partition in which the component resides.
- **port**
  Specifies the port for RADIUS authentication traffic. The default value is **1812**.
- **regex**
  Displays the items that match the regular expression. The regular expression must be preceded by an at sign (@[regular expression]) to indicate that the identifier is a regular expression. See **help regex** for a description of regular expression syntax.

- **secret**
  Specifies the secret key the system uses to encrypt and decrypt packets sent or received from the server. This option is required.
- **server**
  Specifies the host name or IP address of the RADIUS server. This option is required.
- **timeout**
  Specifies the timeout value. The default value is **3** seconds.

See Also

create, *delete*, *edit*, glob, *list*, *profile*, *radius*, *virtual*, *modify*, regex, *show*, *tmsh*

ssl-cc-ldap

Configures an SSL client certificate configuration object for remote SSL-based LDAP authorization for client traffic passing through the traffic management system.

Syntax

Configure the **ssl-cc-ldap** component within the **ltm auth** module using the syntax shown in the following sections.

Create/Modify

```
create ssl-cc-ldap [name]
modify ssl-cc-ldap [anme]
    admin-dn [ [name] | none]
    admin-password [none | [password] ]
    cache-size [integer]
    cache-timeout [integer]
    certmap-base [none | [search base] ]
    certmap-key [ [name] | none)
    certmap-user-serial [no | yes]
    description [string]
    group-base [none | [search base] ]
    group-key [ [name] | none]
    group-member-key [[name] | none]
    role-key [ [name] | none]
    search-type [cert | certmap | user]
    secure [no | yes]
    servers
      [add | delete | none | replace-all-with] {
        [ip address ... ]
    }
    user-base [none | [search base] ]
    user-class [ [class] | none]
    user-key [ [key] | none]
    valid-groups
      [add | delete | replace-all-with] {
        [group ... ]
    }
    valid-groups none
    valid-roles
      [add | delete | replace-all-with] {
        [role ... ]
    }
    valid-roles none
edit ssl-cc-ldap [ [ [name] | [glob] | [regex] ] ... ]
    all-properties
    non-default-properties
```

Display

```
list ssl-cc-ldap
list ssl-cc-ldap [ [ [name] | [glob] | [regex] ] ... ]
show running-config ssl-cc-ldap
show running-config ssl-cc-ldap
```

```
[ [ [name] | [glob] | [regex] ] ... ]
  all-properties
  non-default-properties
  one-line
  partition
```

Delete

```
delete ssl-cc-ldap [name]
```

Description

You can use the **ssl-cc-ldap** component to configure SSL client certificate-based remote LDAP authorization for client traffic passing through the traffic management system.

To configure this type of authentication module and create a configuration object:

1. Use the **ssl-cc-ldap** component in the **ltm auth** module to create an SSL client certificate LDAP configuration object.

2. Use the **profile** component in the **ltm auth** module to create an authentication profile in which you specify the following options:

   a) For the **configuration** option, specify the configuration object that you created in Step 1.

   b) For the **defaults-from** option, specify a parent profile (either the default profile named **ssl_cc_ldap** or another custom profile that you created).

Options

- **admin-dn**
  Specifies the distinguished name of an account to which to bind to perform searches. This search account is a read-only account used to do searches. The **admin** account can also be used as the search account. If no admin DN is specified, then no bind is attempted.
  This option is required only when an LDAP database does not allow anonymous searches. The default value is **none**.
- **admin-password**
  Specifies the password for the admin account. See **admin-dn** above. The default value is **none**.
- **cache-size**
  Specifies the maximum size, in bytes, allowed for the SSL session cache. Setting this option to **0** (zero) disallows SSL session caching. The default value is **20000** bytes (20KB).

- **cache-timeout**
  Specifies the number of usable lifetime seconds of negotiable SSL session IDs. When this time expires, a client must negotiate a new session. The default value is **300** seconds.
- **certmap-base**
  Specifies the search base for the subtree used by the certmap search method. A typical search base is: **ou=people,dc=company,dc=com**. The default value is **none**.
- **certmap-key**
  Specifies the name of the certificate map that the certmap search method uses. This name is found in the LDAP database. The default value is **none**.
- **certmap-user-serial**
  Specifies whether the system uses the client certificate's subject or serial number (in conjunction with the certificate's issuer) when trying to match an entry in the certificate map subtree.
  A value of **yes** uses the serial number. A value of **no** uses the subject. The default value is **no**.
- **description**
  User defined description.
- **glob**
  Displays the items that match the **glob** expression. See **help glob** for a description of **glob** expression syntax.
- **group-base**
  Specifies the search base for the subtree used by group searches. Use this option only when specifying the valid-groups option. The typical search base is similar to: **ou=groups,dc=company,dc=com**. The default value is **none**.
- **group-key**
  Specifies the name of the attribute in the LDAP database that specifies the group name in the group subtree. An example of a typical key is cn (common name for the group). The default value is **none**.
- **group-member-key**
  Specifies the name of the attribute in the LDAP database that specifies members (DNs) of a group. A typical key is **member**. The default value is **none**.
- **name**
  Specifies a unique name for the component. This option is required for the commands **create**, **delete**, and **modify**.
- **partition**
  Displays the administrative partition within which the component resides.
- **regex**
  Displays the items that match the regular expression. The regular expression must be preceded by an at sign (@[regular expression]) to indicate that the identifier is a regular expression. See **help regex** for a description of regular expression syntax.

- **role-key**
  Specifies the name of the attribute in the LDAP database that specifies a user's authorization roles. Use this option only when specifying the **valid-roles** option. A typical role key is **authorizationRole**. The default value is **none**.
- **search**
  Specifies the type of LDAP search that is performed based on the client's certificate. Possible values are:
  - **cert**
    Searches for the exact certificate.
  - **certmap**
    Searches for a user by matching the certificate issuer and the certificate serial number or certificate.
  - **user**
    Searches for a user based on the common name found in the certificate. This is the default value.
- **secure**
  Specifies whether the system attempts to use secure LDAP (LDAP over SSL). The alternative to using secure LDAP is to use insecure (clear text) LDAP. Secure LDAP is a consideration when the connection between the BIG-IP system and the LDAP server cannot be trusted. The default value is **no**.
- **servers**
  Specifies a list of LDAP servers you want to search. You must specify a server when you create an SSL client certificate configuration object.
- **user-base**
  Specifies the search base for the subtree used when you select for the **search** option either of the values **user** or **cert**. A typical search base is: **ou=people,dc=company,dc=com**. You must specify a user base when you create an SSL client certificate configuration object. The default value is **none**.
- **user-class**
  Specifies the object class in the LDAP database to which the user must belong to be authenticated. The default value is **none**.
- **user-key**
  Specifies the key that denotes a user ID in the LDAP database (for example, the common key for the **user** option is **uid**). You must specify a user key when you create an SSL client certificate configuration object.
- **valid-groups**
  Specifies a space-delimited list of the names of groups to which the client must belong in order to be authorized (matches against the group key in the group subtree). The client needs to be a member of only one of the groups in the list. The default value is **none**.
- **valid-roles**
  Specifies a space-delimited list of the valid roles that clients must have to be authorized. The default value is **none**.

See Also

create, *delete*, *edit*, glob, *list*, *profile*, *virtual*, *modify*, regex, *show*, *tmsh*

ssl-crldp

Configures a Secure Socket Layer (SSL) Certificate Revocation List Distribution Point (CRLDP) configuration object for implementing SSL CRLDP to manage certificate revocation.

Syntax

Configure the **ssl-crldp** component within the **ltm auth** module using the syntax shown in the following sections.

Create/Modify

```
create ssl-crldp [name]
modify ssl-crldp [name]
    cache-timeout [integer]
    connection-timeout [integer]
    description [string]
    servers
      [add | delete | replace-all-with] {
        [ip address ... ]
    }
    servers [default | none]
    update-interval [integer]
    use-issuer [disabled | enabled]
edit ssl-crldp [ [ [name] | [glob] | [regex] ] ... ]
    all-properties
    non-default-properties
```

Display

```
list ssl-crldp
list ssl-crldp [ [ [name] | [glob] | [regex] ] ... ]
show running-config ssl-crldp
show running-config ssl-crldp
  [ [ [name] | [glob] | [regex] ] ... ]
    all-properties
    non-default-properties
    one-line
    partition
```

Delete

```
delete ssl-crldp [name]
```

Description

CRLDP authentication is a mechanism for checking certificate revocation status for client connections passing through the system. This module is useful when your authentication data is stored on a remote CRLDP server.

To implement a CRLDP authentication module and create an SSL CRLDP configuration object:

1. Use the **crldp-server** component, in the **ltm auth** module, to create a CRLDP server.

2. Use the **ssl-crldp** component in the **ltm auth** module to configure a CRLDP configuration object that references the server you created in Step 1.

3. Use the **profile** component in the **ltm auth** module to create an authentication profile in which you specify the following options:

   a) For the **configuration** option, specify the SSL CRLDP configuration object that you created in Step 2.

   b) For the **defaults-from** option, specify a parent profile (either the default profile named **ssl_crldp** or another custom profile that you created).

Examples

create ssl-crldp my_auth_ssl-crldp

Creates an SSL CRLDP configuration object named **my_auth_ssl-crldp**.

delete ssl-crldp my_auth_ssl-crldp

Deletes the SSL CRLDP configuration object named **my_auth_ssl-crldp**.

Options

- **cache-timeout**
  Specifies the number of seconds that CRLs are cached. The default value is **86400** (24 hours).
- **connection-timeout**
  Specifies the number of seconds before the connection times out. The default value is **15**.
- **description**
  User defined description.
- **glob**
  Displays the items that match the **glob** expression. See **help glob** for a description of **glob** expression syntax.
- **name**
  Specifies a unique name for the component. This option is required for the commands **create**, **delete**, and **modify**.

- **partition**
  Displays the administrative partition within which the component resides.
- **regex**
  Displays the items that match the regular expression. The regular expression must be preceded by an at sign (@[regular expression]) to indicate that the identifier is a regular expression. See **help regex** for a description of regular expression syntax.
- **servers**
  Specifies a host name or IP address for the secure CRLDP server. This option is required. The default value is **none**.
- **update-interval**
  Specifies an update interval for CRL distribution points that ensures that CRL status is checked at regular intervals, regardless of the CRL timeout value. This helps to prevent CRL information from becoming outdated before the BIG-IP system checks the status of a certificate. The default value is **0** (zero), which indicates an internal default value is active.
- **use-issuer**
  Specifies whether the system extracts the CRL distribution point from the client certificate. The default value is **disabled**.

See Also

create, *delete*, *edit*, glob, *list*, *profile*, *crldp-server*, *virtual*, *modify*, regex, *show*, *tmsh*

ssl-ocsp

Configures OCSP authentication for client traffic passing through the traffic management system.

Syntax

Configure the **ssl-ocsp** component within the **ltm auth** module using the syntax shown in the following sections.

Create/Modify

```
create ssl-ocsp [name]
modify ssl-ocsp [name]
    description [string]
    responders
      [add | delete | replace-all-with] {
        [name]...
    }
    responders [default | none]
edit ssl-ocsp [ [ [name] | [glob] | [regex] ] ... ]
    all-properties
    non-default-properties
```

Display

```
list ssl-ocsp
list ssl-ocsp [ [ [name] | [glob] | [regex] ] ... ]
show running-config ssl-ocsp
show running-config ssl-ocsp
  [ [ [name] | [glob] | [regex] ] ... ]
    all-properties
    non-default-properties
    one-line
    partition
```

Delete

```
delete ssl-ocsp [name]
```

Description

Online Certificate Status Protocol (OCSP) is an industry-standard protocol that offers an alternative to a certificate revocation list when using public-key technology. To implement an SSL OCSP authentication module, you must create the following objects: one or more OCSP responder objects, an SSL OCSP configuration object, and an SSL OCSP profile.

To implement an SSL OCSP authentication module and create an SSL OCSP configuration object:

1. Use the **ocsp-responder** component in the **ltm auth** module to configure an OCSP responder object.

2. Use the **ssl-ocsp** component in the **ltm auth** module to configure an SSL OCSP configuration object to which you add the OCSP responder object that you created in Step 1.

3. Use the **profile** component in the **ltm auth** module to create an authentication profile in which you specify the following options:

   a) For the **configuration** option, specify the SSL OCSP configuration object that you created in Step 2.

   b) For the **defaults-from** option, specify a parent profile (either the default OCSP Responder profile named **ssl_ocsp** or another custom profile that you created).

Examples

create ssl-ocsp my_auth_ssl-ocsp

Creates an SSL OCSP configuration object named **my_auth_ssl-ocsp**.

delete ssl-ocsp my_auth_ssl-ocsp

Deletes the SSL OCSP configuration object named **my_auth_ssl-ocsp**.

Options

- **description**
  User defined description.
- **glob**
  Displays the items that match the **glob** expression. See **help glob** for a description of **glob** expression syntax.
- **name**
  Specifies a unique name for the component. This option is required for the commands **create**, **delete**, and **modify**.
- **partition**
  Displays the administrative partition within which the component resides.

- **regex**
  Displays the items that match the regular expression. The regular expression must be preceded by an at sign (@[regular expression]) to indicate that the identifier is a regular expression. See **help regex** for a description of regular expression syntax.
- **responders**
  Specifies a list of OCSP responders that you configured using the **ocsp-responder** component in the **ltm auth** module.

See Also

create, *delete*, *edit*, glob, *list*, *profile*, *ocsp-responder*, *virtual*, *modify*, regex, *show*, *tmsh*

tacacs

Configures a TACACS+ configuration component for implementing remote TACACS+-based client authentication.

Syntax

Configure the **tacacs** component within the **ltm auth** module using the syntax shown in the following sections.

Create/Modify

```
create tacacs [name]
modify tacacs [name]
    accounting [send-to-all-servers | send-to-first-server]
    authentication [use-all-servers | use-first-server]
    debug [disabled | enabled]
    description [string]
    encryption [disabled | enabled]
    protocol [none | [protocol] ]
    secret [ "[string]" ]
    servers
      [add | delete | replace-all-with] {
        [hostname ... ] | [ip address ... ]
    }
    service [ [name] | none] ]
edit tacacs [ [ [name] | [glob] | [regex] ] ... ]
    all-properties
    non-default-properties
```

Display

```
list tacacs
list tacacs [ [ [name] | [glob] | [regex] ] ... ]
show running-config tacacs
show running-config tacacs [ [ [name] | [glob] | [regex] ] ... ]
    all-properties
    non-default-properties
    one-line
    partition
```

Delete

```
delete tacacs [name]
```

Description

Using a TACACS+ configuration object and profile, you can implement the TACACS+ authentication module as the mechanism for authenticating client connections passing through the BIG-IP Local Traffic Manager

system. You use this module when your authentication data is stored on a remote TACACS+ server. In this case, client credentials are based on basic HTTP authentication (that is, user name and password).

To implement a TACACS+ authentication module and create a TACACS configuration object:

1. Use the **tacacs** component in the **ltm auth** module to configure a TACACS+ configuration object.

2. Use the **profile** component in the **ltm auth** module to create an authentication profile in which you specify the following options:

   a) For the **configuration** option, specify the TACACS+ configuration object that you created in Step 1.

   b) For the **defaults-from** option, specify a parent profile (either the default TACACS+ profile named **tacacs** or another custom profile that you created).

Examples

create tacacs my_tacacs_auth secret "This is the secret" servers add {my_tacacs_server} encryption enabled

Enables encryption for TACACS+ packets.

create tacacs my_tacacs_auth secret "This is the secret" servers add { my_tacacs_server1 my_tacacs_server2 } accounting send-to-all-servers

Provides the ability to send accounting start and stop packets to all servers

Options

- **accounting**
  If multiple TACACS+ servers are defined and pluggable authentication module (PAM) session accounting is available, specifies where the system sends accounting start and stop packets. Possible values are:
  - **send-to-all-servers**
    Sends to all servers.
  - **send-to-first-server**
    Sends to the first available server.
- **authentication**
  Specifies when to use the secret key supplied for the **secret** option. This option is required. The options are:
  - **use-all-servers**
    Use the secret key with all servers.

  - **use-first-server**
    Use the secret key with the first available server.

- **debug**
  Enables syslog-ng debugging information at LOG DEBUG level. F5 Networks does not recommend this option for normal use. The default value is **disabled**.
- **description**
  User defined description.
- **encryption**
  Enables or disables encryption of TACACS+ packets. F5 Networks recommends this option for normal use. The default value is **enabled**.
- **glob**
  Displays the items that match the **glob** expression. See **help glob** for a description of **glob** expression syntax.
- **name**
  Specifies a unique name for the component. This option is required for the commands **create**, **delete**, and **modify**.
- **partition**
  Displays the administrative partition within which the component resides.
- **protocol**
  Specifies the protocol associated with the value specified in the **service** option, which is a subset of the associated service being used for client authorization or system accounting.
- **regex**
  Displays the items that match the regular expression. The regular expression must be preceded by an at sign (@[regular expression]) to indicate that the identifier is a regular expression. See **help regex** for a description of regular expression syntax.
- **secret**
  Sets the secret key used to encrypt and decrypt packets sent or received from the server. This option is required.
- **servers**
  Specifies the host name or IP address of the TACACS+ server. This option is required.
- **service**
  Specifies the name of the service that the user is requesting to be authenticated to use. Identifying the service enables the TACACS+ server to behave differently for different types of authentication requests. This option is required.

See Also

create, *delete*, *edit*, glob, *list*, *profile*, *virtual*, *modify*, regex, *show*, *tmsh*,

51

ltm classification

- Introducing the ltm classification module
- Alphabetical list of components

Introducing the ltm classification module

You can use the tmsh components that reside within the ltm classification module to configure classification signatures, keys, and so on. For more information about the tmsh hierarchical structure, see Chapter 2, *Understanding and Using the Traffic Management Shell*.

Alphabetical list of components

The remainder of this chapter lists the tmsh components that are available in the ltm classification module.

application

Configures a custom classification application.

Syntax

Configure the **application** within the **ltm classification** module using the syntax shown in the following sections.

Create/Modify

```
create application [name]
    app-service [[string] | none]
    description [string]
    application-id [integer]
    status [enabled | disabled]
    category [name]
modify application [name]
    app-service [[string] | none]
    description [string]
    status [enabled | disabled]
    category [name]
edit application [ [ [name] | [glob] | [regex] ] ... ]
    all-properties
    non-default-properties
```

Display

```
list application
list application [ [all] | [name] ]
show running-config application
show running-config application [ [all] | [name] ]
    all-properties
    non-default-properties
    one-line
    partition
```

Delete

```
delete application [name]
```

Note

All referring classification-filters (to this application) need to be deleted first; otherwise an error will be reported. Predefined applications cannot be deleted.

Description

You can use the **application** component to create, modify, delete, and display classification application.

Examples

create application my_app { application-id 8192 status enabled category my_cat }

Creates a new application named **my_app**.

modify application my_app { status disabled category Web description "My description." }

Modify an application named **my_app**.

list application

Displays all created applications.

delete application my_app

Deletes the application named **my_app**.

Options

- **app-service**
  Specifies the name of the application service to which the object belongs. The default value is **none**. **Note:** If the **strict-updates** option is **enabled** on the application service that owns the object, you cannot modify or delete the object. Only the application service can modify or delete the object.
- **description**
  User defined description.
- **application-id**
  Identifies the application. This is set during creation and cannot be changed. Identifiers must be unique across predefined and user-defined applications. Predefined application-ids must be in numeric range [0, 8192), and user defined application-ids must be in numeric range [8192, 16384).
- **status**
  Indicates if this application is enabled or disabled in result of the classification engine.
- **category**
  Refers to classification category. The referred category [name] should exist already; otherwise an error will be reported.

See Also

create, *modify*, *delete*, *list*, *show*, *tmsh*, *ltm classification*, *policy*

category

Configures a custom classification category.

Syntax

Configure the **category** within the **ltm classification** module using the syntax shown in the following sections.

Create/Modify

```
create category [name]
    app-service [[string] | none]
    description [string]
    category-id [integer]
    state [enabled | disabled]
    irule-event [enabled | disabled]
modify category [name]
    app-service [[string] | none]
    description [string]
    state [enabled | disabled]
    irule-event [enabled | disabled]
edit category [ [ [name] | [glob] | [regex] ] ... ]
    all-properties
    non-default-properties
```

Display

```
list category
list category [ [all] | [name] ]
show running-config category
show running-config category [ [all] | [name] ]
    all-properties
    non-default-properties
    one-line
    partition
```

Delete

```
delete category [name]
```

Note

All referring applications/classification-filters (to this category) need to be deleted first; otherwise an error will be reported. Predefined categories cannot be deleted.

Description

You can use the **category** component to create, modify, delete, and display classification category.

Examples

create category my_cat { category-id 20480 state enabled irule-event disabled }

Creates a new category named **my_cat**.

modify category my_cat { state disabled irule-event enabled description "My description." }

Modify a category named **my_cat**.

list category

Displays all created categories.

delete category my_cat

Deletes the category named **my_cat**.

Options

- **app-service**
  Specifies the name of the application service to which the object belongs. The default value is **none**. **Note:** If the **strict-updates** option is **enabled** on the application service that owns the object, you cannot modify or delete the object. Only the application service can modify or delete the object.
- **description**
  User defined description.
- **category-id**
  Identifies the category. This is set during creation and cannot be changed. Identifiers must be unique across predefined and user-defined categories. Predefined category-ids must be in numeric range [16384, 20480), and user defined category-ids must be in numeric range [20480, 24576).
- **state**
  Indicates if this category is enabled or disabled in result of the classification engine.
- **irule-event**
  Indicates if the irule is enabled or disabled in result of the classification engine.

See Also

create, *modify*, *delete*, *list*, *show*, *tmsh*, *ltm classification*, *policy*

http-signature

Configures a custom classification HTTP signature.

Syntax

Configure the **http-signature** component within the **ltm classification** module using the syntax shown in the following sections.

Create/Modify

```
create http-signature [object identifier] application [app_name] category [cat_name]
modify http-signature [object identifier] application [app_name] category [cat_name]
    app-service [[string] | none]
    req-key-values [ [add | del | modify | replace-all-with] {
      [ Content-Type  {value [value_name]} |
        Host          {value [value_name]} |
        Referer       {value [value_name]} |
        User-Agent    {value [value_name]} |
        host          {value [value_name]} |
        hostprefix    {value [value_name]} |
        uri           {value [value_name]} |
        custom_key1   {value [value_name]} |
        custom_key2   {value [value_name]} |
      ] | none]
    resp-key-values [ [add | del | modify | replace-all-with] {
      [ Content-Type  {value [value_name]} |
        customem_key1 {value [value_name]} |
        customem_key2 {value [value_name]} |
      ] | none]
edit http-signature [object identifier | all]
    all-properties
    non-default-properties
```

Display

```
list http-signature
list http-signature [all | object identifier]
show running-config http-signature
show running-config http-signature [all | object identifier]
    all-properties
    non-default-properties
    one-line
```

Delete

```
delete http-signature [all | object identifier]
```

Description

You can use the **http-signature** component to create, delete, and display a classification HTTP signature profile that combines categories and key values of interest. It matches the HTTP traffic with key values defined in the signature. If there is a match, the corresponding **application-name** will be used to identify it.

Examples

create http-signature testSig application gnutella category p2p req-key-values add {User-Agent {value gnutella}}

Creates an HTTP signature named **testSig** of application type **gnutella** and category **p2p** and adds an HTTP Request key of **User-Agent** and a value of **gnutella**.

list http-signature

Displays all HTTP signatures.

list http-signature [object identifier]

Displays the HTTP signatures uniquely identified by **object identifier**.

delete http-signature testSig

Deletes an HTTP signature named **testSig**.

delete http-signature all

Deletes all HTTP signatures.

Options

- **app-service**
  Specifies the name of the application service to which the http-signature belongs. The default value is **none**. **Note:** If the **strict-updates** option is **enabled** on the application service that owns the object, you cannot modify or delete the http-signature. Only the application service can modify or delete the http-signature.
- **application**
  Allows the user to specify an application name. This field can be reused by other signatures as well.
- **category**
  Allows the user to specify a category with the HTTP signature. The specified category could be one of the predefined ones (for example: All, Encrypted, Web, Audio, P2P, video) or a user-specified category that was previously defined.
- **object identifier**
  Specifies a unique identifier for the http-signature. This option is required for the **create http-signature** command.

- **req-key-values**
  Allows the user to create one or more HTTP Request Key/Value pairs. Custom keys must first be created by using create classification key.
- **resp-key-values**
  Allows the user to create one or more HTTP Response Key/Value pairs. Custom keys must first be created by using **create classification key**.

Note

Host, hostprefix, User-Agent, and uri cannot be added to resp-key-values.

See Also

create, *modify*, *edit*, *delete*, *list*, *show*, *tmsh*, *ltm classification*

key

Configures a custom classification key.

Syntax

Configure the **key** within the **ltm classification** module using the syntax shown in the following sections.

Create

```
create key [object identifier]
    app-service [[string] | none]
    priority [integer]
```

Display

```
list key
list key [all | object identifier]
show running-config key
show running-config key [all | object identifier]
    all-properties
    non-default-properties
    one-line
```

Delete

```
delete key [object identifier]
```

Description

You can use the **key** component to create, delete, and display a classification key profile. Host, hostprefix, uri, User-Agent, Content-Type, and Content-Length are system-defined keys and cannot be deleted.

Priority specifies the order in which keys will be given preference. Priority can be any integer starting from 6 (six). Priority numbers 0 (zero) through 5 (five) are system-defined cannot be modified.

If no priority is specified, the next available priority number will be assigned.

For example, if there are two keys K2 and K1 with priority set as 9 (nine) and 10 (ten), there are two signatures S1 {K1:V1} and S2 {K2: V2}, and if HTTP traffic contains the pattern K1:V1 and K2:V2, then the S2 Signature will be matched for this traffic.

Priority is used to resolve conflicts among signatures. If the user does not specify a priority number, the next available priority number will be assigned automatically.

Although you can modify keys, there is no validation check to ensure that all keys have unique priorities. Keys need to have unique priority numbers.

You can create up to a maximum of 225 custom-defined keys.

Examples

create key my_key

Creates a new custom classification key named **my_key**.

create key my_key priority 10

Creates a new custom classification key named **my_key** with priority 10.

modify key my_key priority 6

Changes the custom classification key named **my_key** from priority 10 to priority 6.

list key

Displays all the classification keys.

delete key my_key

Deletes a previously configured classification key named **my_key**.

Options

- **object identifier**
  Specifies a unique identifier for the key. This option is required for the commands **create key** and **delete key**.
- **app-service**
  Specifies the name of the application service to which the classification key belongs. The default value is **none**. **Note:** If the **strict-updates** option is **enabled** on the application service that owns the object, you cannot modify or delete the classification key. Only the application service can modify or delete the classification key.

See Also

list, *show*, *tmsh*, *ltm classification*

policy

Configures an ltm classification url-cat policy. It's comprised of list of urldb feed lists,

Syntax

Configure the **url-cat-policy** component within the **ltm classification** module using the syntax in the following sections.

Create/Modify

Display

```
list url-cat-policy [ [ [name] ]
show running-config url-cat-policy
show running-config url-cat-policy [ [ [name] ]
    all-properties
    non-default-properties
    one-line
    partition
    recursive
```

Display

```
delete url-cat-policy [name]
```

Description

You can use the **url-cat-policy** component to configure a sharable and reusable url categorization database feed coming from local files or download feeds. The url-cat-policy can then be enforced on the configuration object of the type: **ltm virtual**.

Examples

create ltm classification url-cat-policy POL1
feed-lists add { FL1 }
description none
}

Creates a url-cat-policy POL1 with urldb feeds from *FL1* feed lists.

list url-cat-policy

Displays the current list of url-categorization policies contents.

Options

- **app-service**
  Specifies the application service to which the object belongs. The default value is **none**. **Note:** If the **strict-updates** option is **enabled** on the Application Service that owns the object, you cannot modify or delete the object. Only the Application Service can modify or delete the object.
- **description**
  User defined description.
- **partition**
  Displays the administrative partition within which the component resides.
- **feed-lists**
  Adds, deletes, or replaces a feed list. Specifies a list of feed lists (see **ltm classification urldb-feed-list**) against which the packet will be compared.

See Also

create, *edit*, *list*, *modify*, *urldb-feed-list*, *tmsh*

signature-definition

Configure status for classification signature updates.

Syntax

Configure the **signature-definition** component within the **ltm classification** module using the syntax in the following sections.

Display

```
list signature-definition
list signature-definition [ [name] | [glob] | [regex] ]
  all-properties
  non-default-properties
  one-line
  recursive
  last-attempt-automatic-mode [enabled | disabled]
  last-attempt-datetime [date]
  last-attempt-user [string]
  last-update-automatic-mode [enabled | disabled]
  last-update-datetime [date]
  last-update-user [string]
  message [string]
  progress-status [none | success | failure | in-progress]
```

Description

You can use the **signature-definition** component to configure the status for classification signature updates.

Examples

list signature-definition

Displays classification signature update status configuration.

Options

- **last-attempt-automatic-mode**
  Indicates whether the last attempt to update the signature file was done manually or automatically by the system.
- **last-attempt-datetime**
  Indicates the date and time of the last attempt to update the signature file.
- **last-attempt-user**
  Indicates the user who is the last one to attempt to update the signature file.

- **last-update-automatic-mode**
  Indicates whether the last successful signature file update was done manually or automatically by the system. The value of the last-update-automatic-mode may be different from the value of the last-attempt-automatic-mode if the last update attempt fails.
- **last-update-datetime**
  Indicates the date and time of the last successful signature file update. The value of the last-update-datetime is different from the value of the last-attempt-datetime if the last update attempt fails.
- **last-update-user**
  Indicates the user who did the last successful signature file update. The value of the last-update-user may be different from the value of the last-attempt-user if the last update attempt fails.
- **message**
  Indicates the error message when it fails to attempt to update the signature file.
- **progress-status**
  Indicates the progress status when attempting to update the signature file. The options are none, success, failure, and in-progress.

See Also

list, *tmsh*

signature-update-schedule

Configure schedule for classification signature updates.

Syntax

Configure the **signature-update-schedule** component within the **ltm classification** module using the syntax in the following sections.

Modify

```
modify signature-update-schedule [name]
   [auto-update-enabled | auto-update-disabled]
   auto-update-interval [daily | weekly | monthly]
edit signature-update-schedule [name]
  all-properties
  non-default-properties
```

Display

```
list signature-update-schedule
list signature-update-schedule [ [name] | [glob] | [regex] ]
  all-properties
  non-default-properties
  one-line
  recursive
```

Description

You can use the **signature-update-schedule** component to configure schedule for classification signature updates.

Examples

list signature-update-schedule

Displays classification signature update schedule configuration.

modify signature-update-schedule auto-update-enabled auto-update-interval daily

Updates the scheduler for classification signature updates to run once a day.

modify signature-update-schedule auto-update-disabled

Disables the scheduler and allows signatures to update via the browser-based Configuration utility only.

Options

- **app-service**
  Specifies the name of the application service to which the object belongs. The default value is **none**. **Note:** If the **strict-updates** option is **enabled** on the application service that owns the object, you cannot modify or delete the object. Only the application service can modify or delete the object.
- **auto-update-disabled**
  Specifies that the updates scheduler is disabled. The user can update the classification signatures using the browser-based BIG-IP Configuration utility.
- **auto-update-enabled**
  Specifies that the updates scheduler is enabled.
- **auto-update-interval**
  Specifies the auto-update frequency for classification signatures. This attribute will only apply in case auto update is enabled. The default value is **weekly**.

See Also

list, *modify*, *tmsh*

signature-version

Display classification signature version.

Syntax

Display the **signature-version** component within the **ltm classification** module using the syntax in the following sections.

Display

```
list signature-version
  all-properties
  non-default-properties
  one-line
  recursive
```

Description

You can use the **signature-version** component to display versions in classification signature updates.

Examples

list signature-version

Displays classification signature version configuration.

Options

- **cec-filename**
  Indicates the cec library filename in the last updated classification signature.
- **cec-version**
  Indicates the cec library version in the last updated classification signature.
- **classification-version**
  Indicates the classification version in the last updated classification signature.
- **conf-filename**
  Indicates the configuration filename in the last updated classification signature.
- **conf-version**
  Indicates the configuration version in the last updated classification signature.

- **im-version**
  Indicates the im version in the last updated classification signature.
- **qm-protocols-filename**
  Indicates the qosmos protocols filename in the last updated classification signature.
- **qm-protocols-version**
  Indicates the qosmos protocols version in the last updated classification signature.
- **update-time**
  Indicates the update time in the last updated classification signature.

See Also

list, *tmsh*

signatures

Loads signatures for the classification from a file.

Syntax

Loads signatures from a file within the **ltm classification** module using the syntax shown in the following sections.

Load

```
load signatures file [filename]
```

Description

You can use the **signatures** component to load the classification signatures from a file. Only admins can run this command.

You can obtain the latest signature update file (*.im) (if one is available) from http://downloads.f5.com.

For the filename, if no absolute path is specified, the default path /var/local/dpi/signatures/ is used.

Examples

load signatures file my_sig_file.im

Loads signatures from file "my_sig_file.im" under the folder: /var/local/dpi/signatures/.

load signatures file /shared/tmp/new_sig_file.im

Loads signatures from file "new_sig_file.im" under the folder: /shared/tmp/.

See Also

signature-update-schedule, *load*, *tmsh*

update-signatures

Run automatic update for classification signatures.

Syntax

Run the **update-signatures** component within the **ltm classification** module using the syntax in the following sections:

Run

```
run update-signatures
```

Description

You can use the **update-signatures** component to update the classification signatures from F5 download server. Only admins can run this command.

See Also

signature-update-schedule, *run*, *tmsh*

url-category

Configures a custom URL category.

Syntax

Configure the **url-category** within the **ltm classification** module using the syntax shown in the following sections.

Create/Modify

```
create url-category [name]
    app-service [[string] | none]
    description [string]
    url-category-id [integer]
    irule-event [enabled | disabled]
modify url-category [name]
    app-service [[string] | none]
    description [string]
    irule-event [enabled | disabled]
edit url-category [ [ [name] | [glob] | [regex] ] ... ]
    all-properties
    non-default-properties
```

Display

```
list url-category
list url-category [ [all] | [name] ]
show running-config url-category
show running-config url-category [ [all] | [name] ]
    all-properties
    non-default-properties
    one-line
    partition
```

Delete

```
delete url-category [name]
```

Note

All referring url-categorization-filters (to this url-category) need to be deleted first; otherwise an error will be reported. Predefined url-categories cannot be deleted.

Description

You can use the **url-category** component to create, modify, delete, and display classification url-category.

Examples

create url-category my_urlcat { url-category-id 28672 irule-event disabled }

Creates a new url-category named **my_urlcat**.

modify url-category my_urlcat { irule-event enabled description "My description." }

Modify a url-category named **my_urlcat**.

list url-category

Displays all created categories.

delete url-category my_urlcat

Deletes the url-category named **my_urlcat**.

Options

- **app-service**
  Specifies the name of the application service to which the object belongs. The default value is **none**. **Note:** If the **strict-updates** option is **enabled** on the application service that owns the object, you cannot modify or delete the object. Only the application service can modify or delete the object.
- **description**
  User defined description.
- **url-category-id**
  Identifies the url-category. This is set during creation and cannot be changed. Identifiers must be unique across predefined and user-defined categories. Predefined url-category-ids must be in numeric range [24576, 28671), and user defined url-category-ids must be in numeric range [28672-32768).
- **irule-event**
  Indicates if the irule is enabled or disabled in result of the classification engine.

See Also

create, *modify*, *delete*, *list*, *show*, *tmsh*, *ltm classification*, *policy*

urldb-feed-list

Configures a feed-list to be used for URLDB file loads. A *urldb-feed-list* is a list of URL feeds (including local file paths) from where URLDB files are downloaded. These files contain URL categorization information.

Syntax

Configure the **urldb-feed-list** component within the **ltm classification** module using the syntax in the following sections.

Create/Modify

```
create urldb-feed-list [name]
  file [string]
  app-service [name]
  description [string]
```

Display

```
list urldb-feed-list [[name] | all | [property]]
show running-config urldb-feed-list [[name] | all | [property]]
    all-properties
    non-default-properties
    one-line
    partition
    recursive
```

Delete

```
delete urldb-feed-list [[name] | all]
```

Description

You can use the **urldb-feed-list** component to define reusable lists of feeds. You can use a feed list in an **ltm classification url-cat-policy**.

Examples

create urldb-feed-list FL1 { file FILE1 }

Creates a new feed list, "FL1" with URL category information in the file-object FILE1.

Options

- **create**
  Creates a new feed list.

- **delete**
  Deletes the feed list that you specify next, in curly braces ({}).
- **file**
  Specifies the file object containing the URLDB information.
- **app-service**
  Specifies the application service to which the object belongs. The default value is **none**. **Note:** If the **strict-updates** option is **enabled** on the Application Service that owns the object, you cannot modify or delete the object. Only the Application Service can modify or delete the object.
- **description**
  User defined description for this feed list.
- **partition**
  Displays the administrative partition within which the component resides.

See Also

edit, *list*, *modify*, *ltm classification*, *urldb-file*, *tmsh*

urldb-file

Manages a custom URLDB file

Syntax

Configure the **urldb-file** component within the **ltm classification** module using the syntax in the following sections.

Create

```
create urldb-file [name]
  source-path [string]
  app-service [name]
```

Display

```
list urldb-file [[name] | all | [property]]
show running-config urldb-file [[name] | all | [property]]
    all-properties
    one-line
    partition
```

Delete

```
delete urldb-file [[name] | all]
```

Description

You can use the **urldb-file** component to create, list, delete a custom URLDB file. You can use a urldb-file in an **ltm classification urldb-feed-list**.

Examples

create urldb-file FILE1 { source-path file:/shared/images/custom_urldb_1.txt }

Creates a new urldb file object, "FILE1" from the source file /shared/images/custom_urldb_1.txt

Options

- **create**
  Creates a new file object for custom urlcat db.
- **delete**
  Deletes the file object that you specify next, in curly braces ({}).

- **source-path**
  Specifies the location from where the URLDB file object sources the file.
- **app-service**
  Specifies the application service to which the object belongs. The default value is **none**. **Note:** If the **strict-updates** option is **enabled** on the Application Service that owns the object, you cannot modify or delete the object. Only the Application Service can modify or delete the object.
- **description**
  User defined description for this feed list.
- **partition**
  Displays the administrative partition within which the component resides.

See Also

edit, *list*, *ltm classification*, *tmsh*

52

ltm classification stats

- Introducing the ltm classification stats module
- Alphabetical list of components

Introducing the ltm classification stats module

You can use the tmsh components that reside within the ltm classification stats module to view classification statistics for Local Traffic Manager™. For more information about the tmsh hierarchical structure, see Chapter 2, *Understanding and Using the Traffic Management Shell*.

Alphabetical list of components

The remainder of this chapter lists the tmsh components that are available in the ltm classification stats module.

application

Displays and resets classified application statistics.

Syntax

Display statistics for the **application** component within the **ltm classification stats** module using the syntax in the following section.

Display

```
show application
  option:
    (default | exa | gig | kil | meg | peta | raw | tera | yotta | zetta)
```

Description

You can use the **application** component to display classification application statistics. The statistics details are described below:

- **Name**
  Specifies the number of the classified application.
- **Count**
  Specifies a number of classified flows or transactions (in transaction mode) to specific application.
- **LTM Policy**
  Specifies the number of classification decisions by LTM Policy (cpm).
- **Classification Engine**
  Specifies the number of classification decisions by classification engine (CEC).
- **Qosmos iXengine**
  Specifies the number of classification decisions by Qosmos iXengine (ixe).
- **Cache**
  Specifies the number of classification decisions by Cache (srDB).
- **URI Parameter**
  Specifies the number of classification decisions by evaluating HTTP URI query string classification parameter.
- **HTTP Header**
  Specifies the number of classification decisions by using HTTP classification header.
- **iRule**
  Specifies the number of classification decisions by iRule.
- **Bytes in**
  Specifies the bytes in of the classified application.

- **Bytes out**
  Specifies the bytes out of the classified application.
- **Packets in**
  Specifies the packets in of the classified application.
- **Packets out**
  Specifies the packets out of the classified application.

You can reset the classification application statistics using **reset-stats** command.

Examples

show application

Displays the classified application statistics.

reset-stats application

Resets the classified application statistics.

Options

For information about the options that you can use with the command **show**, see **help show**.

See Also

reset-stats, *show*, *tmsh*

url-category

Displays and resets classified url-category statistics.

Syntax

Display statistics for the **url-category** component within the **ltm classification stats** module using the syntax in the following section.

Display

show url-category option: (default | exa | gig | kil | meg | peta | raw | tera | yotta | zetta)

Description

You can use the **url-category** component to display classification url-category statistics. The statistics details are described below:

- **Name**
  Specifies the number of the classified url-category.
- **Count**
  Specifies a number of classified flows or transactions (in transaction mode) to specific url-category.
- **iRule**
  Specifies the number of url-categorization decision by iRule.
- **Customdb**
  Specifies the number of url-categorization decision by custom url database.
- **wrdb**
  Specifies the number of url-categorization decision by webroot database.
- **Bytes in**
  Specifies the bytes in of the classified url-category.
- **Bytes out**
  Specifies the bytes out of the classified url-category.
- **Packets in**
  Specifies the packets in of the classified url-category.
- **Packets out**
  Specifies the packets out of the classified url-category.

You can reset the classification url-category statistics using **reset-stats** command.

Examples

show url-category

Displays the classified url-category statistics.

reset-stats url-category

Resets the classified url-category statistics.

Options

For information about the options that you can use with the command **show**, see **help show**.

See Also

reset-stats, *show*, *tmsh*

53

ltm clientssl

- Introducing the ltm clientssl module
- Alphabetical list of components

Introducing the ltm clientssl module

You can use the tmsh components that reside within the ltm clientssl module to configure client SSL for Local Traffic Manager™. For more information about the tmsh hierarchical structure, see Chapter 2, *Understanding and Using the Traffic Management Shell*.

Alphabetical list of components

The remainder of this chapter lists the tmsh components that are available in the ltm clientssl module.

ocsp-stapling-responses

Deletes the cached OCSP responses on the BIG-IP® system.

Syntax

Use the **ocsp-stapling-responses** component within the **ltm.clientssl** module to manage connections using the following syntax.

Delete

```
delete ocsp-stapling-responses
    virtual [name]
    clientssl-profile [name]
```

Description

You can use the **ocsp-stapling-responses** component to delete the cached OCSP responses based on a specified clientssl profile.

Options

- **virtual**
  Specifies the name of the virtual server that you want to display or delete cached certificates from.
- **clientssl-profile**
  Specifies the name of the clientssl profile that belongs to the virtual selected.

See Also

delete, *tmsh*

54

ltm clientssl-proxy

- Introducing the ltm clientssl-proxy module
- Alphabetical list of components

Introducing the ltm clientssl-proxy module

You can use the tmsh components that reside within the ltm clientssl-proxy module to configure a client-SSL proxy for Local Traffic Manager™. For more information about the tmsh hierarchical structure, see Chapter 2, *Understanding and Using the Traffic Management Shell*.

Alphabetical list of components

The remainder of this chapter lists the tmsh components that are available in the ltm clientssl-proxy module.

cached-certs

Displays and deletes SSL Forward Proxy cached certificates on the BIG-IP® system.

Syntax

Use the **cached-certs** component within the **ltm.clientssl-proxy** module to manage connections using the following syntax.

Display

```
show cached-certs
    virtual [name]
    clientssl-profile [name]
```

Delete

```
delete cached-certs
    virtual [name]
    clientssl-profile [name]
```

Description

You can use the **cached-certs** component to display or delete SSL Forward Proxy cached certificates based on a specified clientssl profile.

Options

- **virtual**
  Specifies the name of the virtual server that you want to display or delete cached certificates from.
- **clientssl-profile**
  Specifies the name of the clientssl profile that belongs to the virtual selected.

See Also

delete, *show*, *tmsh*

55

ltm data-group

- Introducing the ltm data-group module
- Alphabetical list of components

Introducing the ltm data-group module

You can use the tmsh components that reside within the ltm data-group module to create a data-group that contains records that can be used from within an iRule. For more information about the tmsh hierarchical structure, see Chapter 2, *Understanding and Using the Traffic Management Shell*.

Alphabetical list of components

The remainder of this chapter lists the tmsh components that are available in the ltm data-group module.

external

Configures an external class.

Syntax

Configure the **external** data-group within the **ltm data-group** module using the syntax shown in the following sections.

Create/Modify

```
create external [name]
modify external [name]
    app-service [[string] | none]
    description [string]
    external-file-name [ [file name] | none]
    separator [string]
    source-path [URL]
    type [integer | ip | string ]
edit external [ [ [name] | [glob] | [regex] ] ... ]
    all-properties
    non-default-properties
```

Display

```
list external
list external [ [ [name] | [glob] | [regex] ] ... ]
show running-config external
show running-config external [ [ [name] | [glob] | [regex] ] ... ]
    all-properties
    non-default-properties
    one-line
    partition
```

Delete

```
delete external [name]
```

Description

Data groups are lists of data that you define and use with iRules® operators. External data group records are stored in external files that you manage through the **sys file data-group** component. Note that external data groups can be very large, which is one reason why the groups are saved to external files. For example, a phone company may store a list of thousands of phone numbers in an external data group.

You should consider using an internal data group when the number of records is expected to be small.

An external data group acquires its type from the associated data-group file, which can be a list of IP addresses, strings, or integers.

External data groups are lists that specify:

- A data-group file where records are stored
- A description of the class

There are two ways to configure the **external** data-group object:

- Create **external** data-group object, and then specify the source-path and type of the external-file. In one step the external-file will be created within the **sys file data-group** module and **external** data-group within the **ltm data-group** module.
- Create an external-file within the **sys file data-group** module, and then create **external** data-group within the **ltm data-group** module. See **help sys file data-group** for information on creating the data-group file.

Examples

- **create external ext-dg1 external-file-name string.dat description "created for rule xyz"**
  Creates an external data group named **ext-dg1**, with the given description. The records for the data group are loaded from the data-group file **string.dat** previously created in the **sys file data-group** component.
- **create external ext-dg1 description "created for rule xyz" source-path http:/file-server/data-groups/ip.class type ip**
  Downloads the data-group file from the given URL into file-store and creates a data-group file named **ext-dg1** within the **sys file data-group** module. Creates an external data group named **ext-dg1**, with the given description. The records for the data group are loaded from the data-group file **ext-dg1**.
- **create external ext-dg2 source-path file:/shared/save/Test.dat type string**
  Creates a data-group file named **ext-dg2** within the **sys file data-group** module. Creates an external data group named **ext-dg2**. The records for the data group are loaded from the data-group file **ext-dg2**.
- **modify external ext-dg2 description "created for rule abc" source-path file:/shared/save/Test2.dat**
  Downloads the file from the given URL into file-store and updates the source-path of data-group file referenced by external data group **ext-dg2**. Modifies the description of external data group **ext-dg2**.
- **delete external ext-dg1**
  Deletes the external data group named **ext-dg1**. Note: the data-group file referenced by **ext-dg1** is not deleted at this time. If needed, it should be deleted under **sys file data-group** component.

Options

- **app-service**
  Specifies the name of the application service to which the data group belongs. The default value is **none**. **Note:** If the **strict-updates** option is **enabled** on the application service that owns the object, you cannot modify or delete the data group. Only the application service can modify or delete the data group.
- **description**
  User defined description.
- **external-file-name**
  Specifies the data-group file where the records are stored.

◆ Note

*Only source-path or external-file-name may be specified for **external** data-group configuration item.*

- **regex**
  Displays the items that match the regular expression. The regular expression must be preceded by an at sign (@[regular expression]) to indicate that the identifier is a regular expression. See **help regex** for a description of regular expression syntax.
- **separator**
  Specifies a separator to use when defining the data group. The default value is **:=**.
- **source-path** [URL]
  This optional attribute takes a URL.

◆ Note

*Only source-path or external-file-name may be specified for **external** data-group configuration item, for example:*

source-path http://file-server/data-groups/AUL_1.cls

source-path https://file-server/data-groups/CNN.x

source-path ftp://username:password@server/data-groups/latest.class

source-path file:/shared/save/Test.dat

- **type**
  Specifies the kind of data in the group. This option is acquired from the data group file. If the **external** data group is created with external-file that was previously created within the **sys file data-group** module, then **type** option cannot be modified. If the **external** data group is created with source-path option, then **type** should be specified. The value for type could be **integer** or **ip** or **string**.

See Also

create, *delete*, *edit*, glob, *list*, *modify*, regex, *tmsh*

internal

Configures an internal class.

Syntax

Configure the **internal** data-group within the **ltm data-group** module using the syntax shown in the following sections.

Create/Modify

```
create internal [name]
    app-service [[string] | none]
    description [string]
    records [add | delete | modify | replace-all-with] {
      [record key] {
        data [value]
      }
    }
    records none
    type [integer | ip | [string] ]
modify internal [name]
    app-service [[string] | none]
    description [string]
    records [add | delete | modify | replace-all-with] {
      [record key] {
        data [value]
      }
    }
    records none
edit internal [ [ [name] | [glob] | [regex] ] ... ]
    all-properties
    non-default-properties
```

Display

```
list internal
list internal [ [ [name] | [glob] | [regex] ] ... ]
show running-config internal
show running-config internal [ [ [name] | [glob] | [regex] ] ... ]
    all-properties
    non-default-properties
    one-line
    partition
```

Description

Data groups are lists of data that you define and use with iRules® operators. Consider using an external data group if the number of records is expected to be large.

The BIG-IP® system includes a number of predefined lists that you can use. They are:

- aol
- default_accept_language
- images
- private_net

The above lists are located in the file **/config/profile_base.conf**. When you run the **load** command, the system loads these lists; however, unless you have modified the lists, the system does not save the lists to the **bigip.conf** file.

The internal data groups are stored in the **bigip.conf file**.

Internal data groups can be one of three types:

- A list of IP addresses
- A list of strings
- A list of integers

Strings must be surrounded by quotation marks. Numbers can be either positive or negative. These groups define the type of data in the class, which can be IP addresses, strings, or integers>

Examples

create internal MyDG records add { 10.0.0.0 } type ip

Creates an internal data group named **MyDG** that contains a single IP address.

create internal DG2 records add { 192.1.1.255 192.2.1.255 192.3.1.255 } type ip

Creates an internal data group named **DG2** that contains a list of three network addresses: **192.1.1.0/24**, **192.2.1.1/24**, and **192.3.1.1/24**.

create internal MyDG records add { my_key { data my_value } } type string

Creates an internal data group named **MyDG** that contains a single name/value pair.

Options

- **app-service**
  Specifies the name of the application service to which the data group belongs. The default value is **none**. **Note:** If the **strict-updates** option is

enabled on the application service that owns the object, you cannot modify or delete the data group. Only the application service can modify or delete the data group.

- **description**
  User defined description.
- **records**
  Configures the data in the group.
- **regex**
  Displays the items that match the regular expression. The regular expression must be preceded by an at sign (@[regular expression]) to indicate that the identifier is a regular expression. See **help regex** for a description of regular expression syntax.
- **type**
  Specifies the kind of data in the group. The default value is **ip**. This option is required by the command **create**.

See Also

create, *delete*, *edit*, glob, *list*, *modify*, regex, *tmsh*

56

ltm dns

- Introducing the ltm dns module
- Alphabetical list of components

Introducing the ltm dns module

You can use the tmsh components that reside within the ltm dns module to configure DNS for Local Traffic Manager™. For more information about the tmsh hierarchical structure, see Chapter 2, *Understanding and Using the Traffic Management Shell*.

Alphabetical list of components

The remainder of this chapter lists the tmsh components that are available in the ltm dns module.

dns-express-db

Loads the DNS Express data file.

Syntax

```
load dns-express-db
```

Description

The **dns-express-db** component within the **ltm dns** module is used to load the DNS Express data file **/var/db/tmmdns.bin**. The file is only loaded if it has been modified.

Examples

load dns-express-db

Loads the DNS Express file from disk into the running configuration.

See Also

load, *tmsh*

nameserver

Configures DNS nameservers on the BIG-IP® system.

Syntax

Configure the **nameserver** component within the **ltm dns** module using the syntax in the following sections.

Create/Modify

```
create nameserver [name]
modify nameserver [name]
    address [ip address]
    app-service [[string] | none]
    port [unsigned integer]
    route-domain [route-domain name | none]
    tsig-key [tsig-key name | none]
edit nameserver [ [ [name] | [glob] | [regex] ] ... ]
   all-properties
   non-default-properties
reset-stats nameserver
reset-stats nameserver [ [ [name] | [glob] | [regex] ] ... ]
```

Display

```
list nameserver
list nameserver [ [ [name] | [glob] | [regex] ] ... ]
    all-properties
    non-default-properties
    one-line
show nameserver
show nameserver [ [ [name] | [glob] | [regex] ] ... ]
  (default | exa | gig | kil | meg | peta | raw | tera | yotta | zetta)
  global
  field-fmt
```

Delete

```
delete nameserver [name]
```

Description

You can use the **nameserver** component to configure nameservers and to view information about the nameservers.

Examples

create nameserver myNameserver address 127.0.0.1 port 53

Creates the nameserver, **myNameserver**, given the address and port.

list nameserver myNameserver

Displays the properties of the nameserver **myNameserver**.

Options

- **address**
  Specifies the IP address of the nameserver. The default value is 127.0.0.1.
- **app-service**
  Specifies the name of the application service to which the nameserver belongs. The default value is **none**. **Note:** If the **strict-updates** option is **enabled** on the application service that owns the object, you cannot modify or delete the nameserver. Only the application service can modify or delete the nameserver.
- **glob**
  Displays the items that match the **glob** expression. See **help glob** for a description of **glob** expression syntax.
- **name**
  Specifies a unique name for the component. This option is required for the commands **create**, **delete**, and **modify**.
- **port**
  Specifies the service port of the nameserver. The default value is 53.
- **route-domain**
  Specifies the route domain that the nameserver uses for outbound traffic. The default value is the default route domain.
- **tsig-key**
  Specifies the TSIG key used to communicate with this nameserver for zone transfers. If the nameserver is a client, then this TSIG key is used to verify the query and sign the response. If the nameserver is a transfer target for DNS Express nameserver, then this TSIG key should match that of the master nameserver.
- **regex**
  Displays the items that match the regular expression. The regular expression must be preceded by an at sign (@[regular expression]) to indicate that the identifier is a regular expression. See **help regex** for a description of regular expression syntax.

See Also

create, *delete*, *edit*, glob, *list*, *modify*, regex, *show*, *tmsh*

tsig-key

Configures TSIG keys on the BIG-IP® system.

Syntax

Configure the **tsig-key** component within the **ltm dns** module using the syntax in the following sections.

Create/Modify

```
create tsig-key [name]
modify tsig-key [name]
    algorithm [ hmacmd5 | hmacsha1 | hmacsha256 ]
    app-service [[string] | none]
    secret [string]
edit tsig-key [ [ [name] | [glob] | [regex] ] ... ]
   all-properties
   non-default-properties
```

Display

```
list tsig-key
list tsig-key [ [ [name] | [glob] | [regex] ] ... ]
    all-properties
    non-default-properties
    one-line
```

Delete

```
delete tsig-key [name]
```

Description

You can use the **tsig-key** component to configure TSIG keys and to view information about the keys.

Examples

create tsig-key myKey algorithm hmacmd5 secret ABCDEFG

Creates the TSIG key, **myKey**, given the algorithm and secret (both required).

list tsig-key myKey

Displays the properties of the TSIG key **myKey**.

Options

- **algorithm**
  Specifies the algorithm to use to generate the key.
- **app-service**
  Specifies the name of the application service to which the TSIG key belongs. The default value is **none**. **Note:** If the **strict-updates** option is **enabled** on the application service that owns the object, you cannot modify or delete the TSIG key. Only the application service can modify or delete the TSIG key.
- **glob**
  Displays the items that match the **glob** expression. See **help glob** for a description of **glob** expression syntax.
- **name**
  Specifies a unique name for the component. This option is required for the commands **create**, **delete**, and **modify**.
- **regex**
  Displays the items that match the regular expression. The regular expression must be preceded by an at sign (@[regular expression]) to indicate that the identifier is a regular expression. See **help regex** for a description of regular expression syntax.
- **secret**
  Specifies the string representation of the key's shared secret.

See Also

create, *delete*, *edit*, glob, *list*, *modify*, regex, *tmsh*

zone

Configures zones on the BIG-IP® system.

Syntax

Configure the **zone** component within the **ltm dns** module using the syntax in the following sections.

Create/Modify

```
create zone [name]
modify zone [name]
    app-service [[string] | none]
    dns-express-allow-notify [add | delete | none | replace-all-with] {
       [IP Address]
    }
    dns-express-enabled [yes | no]
    dns-express-notify-action [ consume | bypass | repeat ]
    dns-express-notify-tsig-verify [yes | no]
    dns-express-server [server name | none]
    response-policy [yes | no]
    server-tsig-key [tsig-key name | none]
    transfer-clients [add | delete | none | replace-all-with] {
        [server name]
    }
edit zone [ [ [name] | [glob] | [regex] ] ... ]
   all-properties
   non-default-properties
reset-stats zone
reset-stats zone [ [ [name] | [glob] | [regex] ] ... ]
```

Display

```
list zone
list zone [ [ [name] | [glob] | [regex] ] ... ]
    all-properties
    non-default-properties
    one-line
show zone [ [ [name] | [glob] | [regex] ] ... ]
  (default | exa | gig | kil | meg | peta | raw | tera | yotta | zetta)
  field-fmt
```

Delete

```
delete zone [name]
```

Description

You can use the **zone** component to configure and view information about a zone.

Examples

list zone myZone

Displays the properties of the zone named **myZone**.

create zone myZone transfer-clients add { nameserver1 nameserver2 }

Creates a zone named **myZone**, which allows zone data to be transfered to **nameserver1** and **nameserver2**.

Options

- **app-service**
  Specifies the name of the application service to which the zone belongs. The default value is **none**. **Note:** If the **strict-updates** option is **enabled** on the application service that owns the object, you cannot modify or delete the zone. Only the application service can modify or delete the zone.
- **dns-express-allow-notify**
  Specifies a list of IP addresses, in addition to the DNS Zone's DNS-Express Server address, which are allowed to notify the BIGIP of DNS Zone changes. A notify message coming from an IP which is neither the address of the zone's DNS Express server nor an address in this list will be dropped by the BIGIP.
- **dns-express-enabled [yes | no]**
  Specifies whether DNS Express is enabled to process queries for this zone. The default value is **yes**.
- **dns-express-notify-action [consume | bypass | repeat]**
  Action to take when a NOTIFY query is received for a configured zone. Options are **consume**, **bypass**, and **repeat**. Default is **consume**, meaning the NOTIFY query is seen only by DNS Express. **bypass** means the query will NOT go to DNS Express, but any backend DNS resource (subect to DNS profile **unhandled-query-action**). **repeat** means the NOTIFY will go to both DNS Express and any backend DNS resource. If TSIG is configured, the signature is only validated for **consume** and **repeat** actions. NOTIFY responses are assumed to be sent by the backend DNS resource, except when the action is **consume** and DNS Express will generate a response.
- **dns-express-notify-tsig-verify**
  Verify NOTIFY query TSIG for a DNS Express zone. Default is **yes**.
- **dns-express-server**
  Specifies the server from which to retrieve zone information for DNS Express.
- **glob**
  Displays the items that match the **glob** expression. See **help glob** for a description of **glob** expression syntax.

- **name**
  Specifies a unique name for the component. This option is required for the commands **create**, **delete**, and **modify**.

Note

A successful zone transfer must occur before this zone can service DNS requests.

- **regex**
  Displays the items that match the regular expression. The regular expression must be preceded by an at sign (@[regular expression]) to indicate that the identifier is a regular expression. See **help regex** for a description of regular expression syntax.
- **response-policy**
  Specifies if this is a response policy zone. If this is set to yes, this zone may be assigned as an RPZ to a DNS Cache. Default is **no**.
- **server-tsig-key**
  Specifies the server side TSIG key associated with the DNS zone. It should match the TSIG Key associcated with the master name servers.
- **transfer-clients**
  Specifies the nameservers allowed to transfer the zone from BIGIP.

See Also

create, *delete*, *edit*, glob, *list*, *show*, *modify*, regex, *tmsh*

57

ltm dns analytics

- Introducing the ltm dns analytics module
- Alphabetical list of components

Introducing the ltm dns analytics module

You can use the tmsh components that reside within the ltm dns analytics module to set up DNS listeners on LTM. The DNS listeners collect DNS-traffic data for analysis. For more information about the tmsh hierarchical structure, see Chapter 2, *Understanding and Using the Traffic Management Shell*.

Alphabetical list of components

The remainder of this chapter lists the tmsh components that are available in the ltm dns analytics module.

global-settings

Configures the global settings of all DNS listeners on the BIG-IP® system.

Syntax

Configure the **global-settings** DNS listeners within the **ltm dns analytics** module using the syntax in the following sections.

Modify

```
modify global-settings
    collect-client-ip [enabled | disabled]
    collect-query-name [enabled | disabled]
```

Display

```
list global-settings
list global-settings
    all-properties
    non-default-properties
    one-line
```

Description

You can use the **global-settings** component to configure and view information about the global settings of all DNS listeners.

Examples

list global-settings all-properties

Displays the global settings for the DNS listeners on the BIG-IP system.

Options

- **collect-client-ip**
  When enabled, the client IP addresses of DNS queries will be collected and stored in analytics database. The default value is **enabled**.
- **collect-query-name**
  When enabled, the domain names of DNS queries will be collected and stored in analytics database. The default value is **enabled**.

See Also

list, *modify*, *tmsh*

58

ltm dns cache

- Introducing the ltm dns cache module
- Alphabetical list of components

Introducing the ltm dns cache module

You can use the tmsh components that reside within the ltm dns cache module to configure DNS caches for Local Traffic Manager™. For more information about the tmsh hierarchical structure, see Chapter 2, *Understanding and Using the Traffic Management Shell*.

Alphabetical list of components

The remainder of this chapter lists the tmsh components that are available in the ltm dns cache module.

global-settings

Configures the global settings of all DNS caches on the BIG-IP® system.

Syntax

Configure the **global-settings** DNS cache component within the **ltm dns cache** module using the syntax in the following sections.

Create/Modify

```
modify global-settings [name]
    cache-maximum-ttl [integer]
    cache-minimum-ttl [integer]
    resolver-edns-buffer-size [integer]
edit global-settings [ [ [name] | [glob] | [regex] ] ... ]
   all-properties
   non-default-properties
```

Display

```
list global-settings
list global-settings [ [ [name] | [glob] | [regex] ] ... ]
    all-properties
    non-default-properties
    one-line
```

Description

You can use the **global-settings** component to configure and view information about the global settings of all DNS caches.

Examples

list global-settings all-properties

Displays the global settings for the DNS caches on the BIG-IP system.

Options

- **cache-maximum-ttl**
  Specifies the number of seconds after which you want the BIG-IP system to re-query for resource records. This setting allows the BIG-IP system to re-query for resource records sooner than the owner of the records intended.

- **cache-minimum-ttl**
  Specifies the minimum number of seconds you want the BIG-IP system to cache DNS resource records. This setting allows the BIG-IP system to cache resource records longer than the owner of the records intended.
- **glob**
  Displays the items that match the **glob** expression. See **help glob** for a description of **glob** expression syntax.
- **regex**
  Displays the items that match the regular expression. The regular expression must be preceded by an at sign (@[regular expression]) to indicate that the identifier is a regular expression. See **help regex** for a description of regular expression syntax.
- **resolver-edns-buffer-size [integer]**
  Specifies the number of bytes you want the BIG-IP system to advertise as the EDNS buffer size in UDP queries.

See Also

edit, glob, *list*, *modify*, regex, *tmsh*

resolver

Configures a DNS cache with a resolver on the BIG-IP® system.

Syntax

Configure the **resolver** DNS cache component within the **ltm dns cache** module using the syntax in the following sections.

Create/Modify

```
create resolver [name]
modify resolver [name]
    allowed-query-time [integer]
    answer-default-zones [yes | no]
    app-service [[string] | none]
    forward-zones [add | delete | modify | replace-all-with] {
      [ [zone-name] ] {
          nameservers [add | delete | replace-all-with] {
            [ [IPv4address:port] | [IPv6address.port] ]
          }
          nameservers none
    }
    forward-zones none
    local-zones [ [none] |
          [ { { name [dname] type [type] records [none | add { [RR string] ...} ] } ...
} ] ]
    max-concurrent-queries [integer]
    max-concurrent-tcp [integer]
    max-concurrent-udp [integer]
    msg-cache-size [integer]
    nameserver-cache-count [integer]
    randomize-query-name-case [yes | no]
    response-policy-zones [add | delete | modify] {
      [zone-name] {
         action [nxdomain | walled-garden]
         walled-garden [local-zone]
      }
    }
    response-policy-zones none
    root-hints {
       { [IP address] ... }
    }
    route-domain [name]
    rrset-cache-size [integer]
    unwanted-query-reply-threshold [integer]
    use-ipv4 [yes | no]
    use-ipv6 [yes | no]
    use-tcp [yes | no]
    use-udp [yes | no]
```

Display

```
list resolver
list resolver [ [ [name] | [glob] | [regex] ] ... ]
    all-properties
    non-default-properties
```

```
    one-line
show resolver
show resolver [name]
```

Delete

```
delete resolver [name]
```

Description

You can use the **resolver** component to configure and view information about a recursive-resolving DNS cache. A resolver cache performs recursive resolution to fill its cache.

Important

When sizing caches, consider the total amount of memory available and how you wish to allocate memory for DNS caching. Note that cache sizing values are per-TMM process; therefore, a platform with eight TMMs consumes the amount of memory set for the RRset cache times eight.

Examples

list resolver myCache

Displays the properties of the recursive-resolving DNS cache **myCache**.

modify resolver myCache local-zones { { name lz.example.net records add { "lz.example.net 60 IN A 127.0.0.1" "www.lz.example.net 300 IN A 127.0.0.2" } } }

Modifies DNS cache **myCache** by adding a local-zone **lz.example.net** with 2 resource records.

Options

- **allowed-query-time**
  Specifies the time allowed for a query to stay in the queue before it is replaced by a new query when the number of concurrent distinct queries exceeds the limit. The default value is 200 milliseconds.
- **answer-default-zones**
  Specifies whether the resolver cache answers queries for default zones: localhost, reverse 127.0.0.1 and ::1, and AS112 zones. The default value is **no**.
- **app-service**
  Specifies the name of the application service to which the object belongs. The default value is **none**. **Note:** If the **strict-updates** option is **enabled** on the application service that owns the object, you cannot modify or delete the object. Only the application service can modify or delete the object.

- **forward-zones**
  Adds, deletes, modifies, or replaces a set of forward zones on a DNS Cache, by specifying zone name(s). A given zone name should only use the symbols allowed for a fully qualified domain name (FQDN), namely ASCII letters **a** though **z**, digits **0** through **9**, hyphen **-**, and period **.**. For example **site.example.com** would be a valid zone name.
  A DNS Cache configured with a forward zone will forward any queries that result in a cache-miss (the answer was not available in the cache) and which match a configured zone name, to the nameserver specified on the zone. If no nameservers are specified on the zone, an automatic SERVFAIL is returned. When a forward zone's nameserver returns a valid response to the DNS Cache, that response is cached and then returned to the requestor.
  - **nameservers**
    Adds, deletes, modifies, or replaces a set of nameservers in a forward zone on a DNS Cache. A nameserver is represented by an **IPaddress** and **port** in the format **[IPv4:port]** or **[IPv6.port]**, for example **10.10.10.10:53** or **2001::1:ff.53**, respectively.
    If more than one nameserver is listed for a given forward zone, a matching query will be sent to the nameserver that is currently deemed the most responsive (based on RTTs). If no response is received within a certain window of time, the DNS Cache will resend the query to another nameserver with an increased wait window until a response is received.
- **glob**
  Displays the items that match the **glob** expression. See **help glob** for a description of **glob** expression syntax.
- **local-zones**
  Zones and associated resource records for which the cache will provide Authoritative responses. Default is empty. This is intended for small, simple authoritative data configurations.
  The local-zone **name** must be fully qualified and should be the apex of the zone. The local-zone **type** may be one of the following: **deny**, **refuse**, **static**, **transparent**, **type-transparent**, or **redirect**. Zero or more resource records must be fully specified: name, ttl, class, type, and record data, separated by spaces, and within double quotes. For example, "www.example.net. 300 IN A 1.2.3.4".
  For all local-zones types, if the DNS query matches, it is answered Authoritatively. How a non-matching query is handled depends on the local-zone **type**.
  deny drops the query.
  refuse sends a REFUSED response.
  static sends either a NoData or NXDOMAIN response (includes SOA if present in local-zone).
  transparent performs regular cache operation (i.e. transparent pass-through or iterative resolution) except for those query names which would result in NoData. This is the default local-zone **type**.
  type-transparent Same as **transparent** but does not return NoData.
  redirect returns responses with zone suffix record(s) for queries beneath that suffix. For example, a local-zone for example.com and a single A

record for that name; queries for www.example.com or abc.www.example.com would return the single A record (both have the same suffix).

- **max-concurrent-queries**
  Specifies the maximum number of concurrent distinct queries used by the resolver. A query is identified by query name, type and class. If the number of distinct queries exceeds this limit, the resolver replaces the earliest query in the queue with the new query if it has been in the queue longer than the allowed time. The default value is **1024**.
- **max-concurrent-tcp**
  Specifies the maximum number of concurrent TCP flows used by the resolver. The default value is **20**.
- **max-concurrent-udp**
  Specifies the maximum number of concurrent UDP flows used by the resolver. The default value is **8192**.
- **msg-cache-size**
  Specifies the maximum size in bytes of the DNS message cache. The default value is **1048576**.
  The BIG-IP system caches the messages in a DNS response in the message cache. After the maximum size of the cache is reached, when new or refreshed content is added to the cache, the expired and older content is removed from the cache. A higher maximum size allows more DNS responses to be cached and increases the cache hit percentage. A lower maximum size forces earlier eviction of cached content, but can lower the cache hit percentage.
- **name**
  Specifies a unique name for the component. This option is required for the commands **create**, **delete**, and **modify**.
- **nameserver-cache-count**
  Specifies the maximum number of DNS nameservers for which the BIG-IP system caches connection and capability data. The default value is **16536** entries.
- **randomize-query-name-case**
  When enabled, the resolver randomizes the case of query names. The default value is **yes**.
- **regex**
  Displays the items that match the regular expression. The regular expression must be preceded by an at sign (@[regular expression]) to indicate that the identifier is a regular expression. See **help regex** for a description of regular expression syntax.
- **response-policy-zones**
  Adds, deletes or modifies the response policy zone to be used by this DNS Cache. Only a DNS Express zone configured as a response policy zone can be added.
  The query name of a recursive DNS request without DNSSEC enabled is queried against the data in the response policy zone. If a match is found, the configured response policy action is taken.

- **action**
  The action to take upon a match. **nxdomain** results in an NXDOMAIN response given to the client. **walled-garden** results in a response with a CNAME to the walled-garden zone and an A or AAAA response matching the DNS query type. The default action is **nxdomain**.
- **walled-garden**
  A local zone configured in this cache that contains an A and/or AAAA record. This is typically used to redirect a user that requests resolution of a name contained in the RPZ database to a local server. This local server can display a message to the user and/or record the connection. Only A/AAAA/ANY requests are redirected, a request for any other type is answered with a NoData response. If a request is received for type A or AAAA but there are no records of that type configured, a NoData response is returned instead.

◆ **root-hints**
Specifies the IP addresses of DNS servers that the BIG-IP system considers authoritative for the DNS root nameservers.

Important

By default, the BIG-IP system uses the DNS root nameservers published by InterNIC.
Caution: *When you add DNS root nameservers, the BIG-IP system no longer uses the default nameservers published by InterNIC, but instead uses the nameservers you add as authoritative for the DNS root nameservers.*

◆ **route-domain**
Specifies the route domain the resolver uses for outbound traffic. The default value is the default route domain.

◆ **rrset-cache-size**
Specifies the maximum size in bytes of the resource records set cache. The default value is **10485760**.
The BIG-IP system caches the supporting records in a DNS response in the resource record cache. After the maximum size of the cache is reached, when new or refreshed content is added to the cache, the expired and older content is removed from the cache. A higher maximum size allows more DNS responses to be cached and increases the cache hit percentage. A lower maximum size forces earlier eviction of cached content, but can lower the cache hit percentage.

◆ **unwanted-query-reply-threshold**
The system always rejects unsolicited replies. The default value of **0** (off) indicates the system does not generate SNMP traps or log messages when rejecting unsolicited replies.
Change the default value to monitor for unsolicited replies. This alerts you to a potential security attack, such as cache poisoning or DOS. For example, if you specify a value of 1,000,000, each time the system receives 1,000,000 unsolicited replies, it generates an SNMP trap and log message. The default value is **0** (off).

- **use-ipv4**
  When enabled, the resolver sends DNS queries to IPv4 addresses. The default value is **yes**.
- **use-ipv6**
  When enabled, the resolver sends DNS queries to IPv6 addresses. The default value is **yes**.
- **use-tcp**
  When enabled, the resolver can send queries over the TCP protocol. The default value is **yes**.
- **use-udp**
  When enabled, the resolver can send queries over the UDP protocol. The default value is **yes**.

See Also

create, *delete*, *edit*, glob, *list*, *transparent*, *validating-resolver*, *show*, *modify*, regex, *tmsh*

transparent

Configures a DNS cache without a resolver on the BIG-IP® system.

Syntax

Configure the **transparent** DNS cache component within the **ltm dns cache** module using the syntax in the following sections.

Create/Modify

```
create transparent [name]
modify transparent [name]
    answer-default-zones [yes | no]
    app-service [[string] | none]
    dnssec-on-miss [yes | no]
    local-zones [ [none] |
          [ { { name [dname] type [type] records [none | add { [RR string] ...} ] } ...
} ] ]
    msg-cache-size [integer]
    response-policy-zones [add | delete | modify] {
      [zone-name] {
         action [nxdomain | walled-garden]
         walled-garden [local-zone]
      }
    }
    response-policy-zones none
    rrset-cache-size [integer]
```

Display

```
list transparent
list transparent [ [ [name] | [glob] | [regex] ] ... ]
    all-properties
    non-default-properties
    one-line
show transparent
show transparent [name]
```

Delete

```
delete transparent [name]
```

Description

You can use the **transparent** component to configure and view information about a transparent DNS cache. A transparent cache does not perform recursive resolution, but instead relies on another DNS resource for this functionality.

Important

When sizing caches, consider the total amount of memory available and how you wish to allocate memory for DNS caching. Note that cache sizing values are per-TMM process; therefore, a platform with eight TMMs consumes the amount of memory set for the RRset cache times eight.

Examples

list transparent myCache

Displays the properties of the transparent DNS cache **myCache**.

modify transparent myCache local-zones { { name lz.example.net records add { "lz.example.net 60 IN A 127.0.0.1" "www.lz.example.net 300 IN A 127.0.0.2" } } }

Modifies DNS cache **myCache** by adding a local-zone **lz.example.net** with 2 resource records.

Options

- **answer-default-zones**
  Specifies whether the resolver cache answers queries for default zones: localhost, reverse 127.0.0.1 and ::1, and AS112 zones. The default value is **no**.
- **app-service**
  Specifies the name of the application service to which the object belongs. The default value is **none**. **Note:** If the **strict-updates** option is **enabled** on the application service that owns the object, you cannot modify or delete the object. Only the application service can modify or delete the object.
- **dnssec-on-miss**
  Specifies whether, on a cache miss, the BIG-IP system forwards queries after adding the DNSSEC OK bit. The default value is **yes**.
- **glob**
  Displays the items that match the **glob** expression. See **help glob** for a description of **glob** expression syntax.
- **local-zones**
  Zones and associated resource records for which the cache will provide Authoritative responses. Default is empty. This is intended for small, simple authoritative data configurations.
  The local-zone **name** must be fully qualified and should be the apex of

the zone. The local-zone **type** may be one of the following: **deny**, **refuse**, **static**, **transparent**, **type-transparent**, or **redirect**. Zero or more resource records must be fully specified: name, ttl, class, type, and record data, separated by spaces, and within double quotes. For example, "www.example.net. 300 IN A 1.2.3.4".
For all local-zones types, if the DNS query matches, it is answered Authoritatively. How a non-matching query is handled depends on the local-zone **type**.
deny drops the query.
refuse sends a REFUSED response.
static sends either a NoData or NXDOMAIN response (includes SOA if present in local-zone).
transparent performs regular cache operation (i.e. transparent pass-through or iterative resolution) except for those query names which would result in NoData. This is the default local-zone **type**.
type-transparent Same as **transparent** but does not return NoData.
redirect returns responses with zone suffix record(s) for queries beneath that suffix. For example, a local-zone for example.com and a single A record for that name; queries for www.example.com or abc.www.example.com would return the single A record (both have the same suffix).

- **msg-cache-size**
  Specifies the maximum size in bytes of the DNS message cache. The default value is **1048576**.
  The BIG-IP system caches the messages in a DNS response in the message cache. After the maximum size of the cache is reached, when new or refreshed content is added to the cache, the expired and older content is removed from the cache. A higher maximum size allows more DNS responses to be cached and increases the cache hit percentage. A lower maximum size forces earlier eviction of cached content, but can lower the cache hit percentage.
- **name**
  Specifies a unique name for the component. This option is required for the commands **create**, **delete**, and **modify**.
- **regex**
  Displays the items that match the regular expression. The regular expression must be preceded by an at sign (@[regular expression]) to indicate that the identifier is a regular expression. See **help regex** for a description of regular expression syntax.
- **response-policy-zones**
  Adds, deletes or modifies the response policy zone to be used by this DNS Cache. Only a DNS Express zone configured as a response policy zone can be added.
  The query name of a recursive DNS request without DNSSEC enabled is queried against the data in the response policy zone. If a match is found, the configured response policy action is taken.
  - **action**
    The action to take upon a match. **nxdomain** results in an NXDOMAIN response given to the client. **walled-garden** results in a

response with a CNAME to the walled-garden zone and an A or AAAA response matching the DNS query type. The default action is **nxdomain**.

- **walled-garden**
  A local zone configured in this cache that contains an A and/or AAAA record. This is typically used to redirect a user that requests resolution of a name contained in the RPZ database to a local server. This local server can display a message to the user and/or record the connection. Only A/AAAA/ANY requests are redirected, a request for any other type is answered with a NoData response. If a request is received for type A or AAAA but there are no records of that type configured, a NoData response is returned instead.

- **rrset-cache-size**
  Specifies the maximum size in bytes of the resource records set cache. The default value is **10485760**.
  The BIG-IP system caches the supporting records in a DNS response in the resource record cache. After the maximum size of the cache is reached, when new or refreshed content is added to the cache, the expired and older content is removed from the cache. A higher maximum size allows more DNS responses to be cached and increases the cache hit percentage. A lower maximum size forces earlier eviction of cached content, but can lower the cache hit percentage.

See Also

create, *delete*, *edit*, glob, *list*, *resolver*, *validating-resolver*, *show*, *modify*, regex, *tmsh*

validating-resolver

Configures a DNS cache with a resolver and validator on the BIG-IP® system.

Syntax

Configure the **validating-resolver** DNS cache component within the **ltm dns cache** module using the syntax in the following sections.

Create/Modify

```
create validating-resolver [name]
modify validating-resolver [name]
    allowed-query-time [integer]
    answer-default-zones [yes | no]
    app-service [[string] | none]
    dlv-anchors {
       { [DNSKEY or DS RR string] ... }
    }
    forward-zones [add | delete | modify | replace-all-with] {
      [ [zone-name] ] {
          nameservers [add | delete | replace-all-with] {
            [ [IPv4address:port] | [IPv6address.port] ]
          }
          nameservers none
    }
    forward-zones none
    ignore-cd [yes | no]
    key-cache-size [integer]
    local-zones [ [none] |
          [ { { name [dname] type [type] records [none | add { [RR string] ...} ] } ...
} ] ]
    max-concurrent-queries [integer]
    max-concurrent-udp [integer]
    max-concurrent-tcp [integer]
    msg-cache-size [integer]
    nameserver-cache-count [integer]
    prefetch-key [yes | no]
    randomize-query-name-case [yes | no]
    response-policy-zones [add | delete | modify] {
      [zone-name] {
         action [nxdomain | walled-garden]
         walled-garden [local-zone]
      }
    }
    response-policy-zones none
    root-hints {
       { [IP address] ... }
    }
    route-domain [name]
 rrset-cache-size [integer]
    trust-anchors {
       { [NDSKEY or DS RR string] ... }
    }
    unwanted-query-reply-threshold [integer]
    use-ipv4 [yes | no]
```

```
    use-ipv6 [yes | no]
    use-tcp [yes | no]
    use-udp [yes | no]
```

Display

```
list validating-resolver
list validating-resolver [ [ [name] | [glob] | [regex] ] ... ]
    all-properties
    non-default-properties
    one-line
show validating-resolver [name]
```

Delete

```
delete validating-resolver [name]
```

Description

You can use the **validating-resolver** component to configure and view information about a validating recursive-resolving DNS cache. A resolving and validating cache performs recursive resolution to fill its cache and uses DNSSEC to ensure the integrity of the data.

Important

When sizing caches, consider the total amount of memory available and how you wish to allocate memory for DNS caching. Note that cache sizing values are per-TMM process; therefore, a platform with eight TMMs consumes the amount of memory set for the resource record set cache times eight.

Examples

list validating-resolver myCache

Displays the properties of the validating recursive-resolving DNS cache **myCache**.

modify validating-resolver myCache local-zones { { name lz.example.net records add { "lz.example.net 60 IN A 127.0.0.1" "www.lz.example.net 300 IN A 127.0.0.2" } } }

Modifies DNS cache **myCache** by adding a local-zone **lz.example.net** with 2 resource records.

Options

- **allowed-query-time**
  Specifies the time allowed for a query to stay in the queue before it is replaced by a new query when the number of concurrent distinct queries exceeds the limit. The default value is 200 milliseconds.

- **answer-default-zones**
  Specifies whether the validating resolver cache answers queries for default zones: localhost, reverse 127.0.0.1 and ::1, and AS112 zones. The default value is **no**.
- **app-service**
  Specifies the name of the application service to which the object belongs. The default value is **none**. **Note:** If the **strict-updates** option is **enabled** on the application service that owns the object, you cannot modify or delete the object. Only the application service can modify or delete the object.
- **dlv-anchors**
  Specifies the DNSKEY or DS resource records the BIG-IP system uses to establish DNSSEC trust with a DLV registry. The resource records must be specified in string format, for example, dig or drill format. The default is **none**.
- **forward-zones**
  Adds, deletes, modifies, or replaces a set of forward zones on a DNS Cache, by specifying zone name(s). A given zone name should only use the symbols allowed for a fully qualified domain name (FQDN), namely ASCII letters **a** though **z**, digits **0** through **9**, hyphen **-**, and period **.**. For example **site.example.com** would be a valid zone name.
  A DNS Cache configured with a forward zone will forward any queries that result in a cache-miss (the answer was not available in the cache) and which match a configured zone name, to the nameserver specified on the zone. If no nameservers are specified on the zone, an automatic SERVFAIL is returned. When a forward zone's nameserver returns a valid response to the DNS Cache, that response is cached and then returned to the requestor.
  - **nameservers**
    Adds, deletes, or replaces a set of nameservers in a forward zone on a DNS Cache. A nameserver is represented by an **IPaddress** and **port** in the format **[IPv4:port]** or **[IPv6.port]**, for example **10.10.10.10:53** or **2001::1:ff.53**, respectively.
    If more than one nameserver is listed for a given forward zone, a matching query will be sent to the nameserver that is currently deemed the most responsive (based on RTTs). If no response is received within a certain window of time, the DNS Cache will resend the query to another nameserver with an increased wait window until a response is received.
- **glob**
  Displays the items that match the **glob** expression. See **help glob** for a description of **glob** expression syntax.
- **ignore-cd**
  When enabled, the system ignores the Checking Disabled setting on client queries, performs validation, and returns only secure answers. The default value is **no**.
- **key-cache-size**
  Specifies the maximum size in bytes of the DNSKEY cache. The default value is **1048576**.

- **local-zones**
  Zones and associated resource records for which the cache will provide Authoritative responses. Default is empty. This is intended for small, simple authoritative data configurations.
  The local-zone **name** must be fully qualified and should be the apex of the zone. The local-zone **type** may be one of the following: **deny**, **refuse**, **static**, **transparent**, **type-transparent**, or **redirect**. Zero or more resource records must be fully specified: name, ttl, class, type, and record data, separated by spaces, and within double quotes. For example, "www.example.net. 300 IN A 1.2.3.4".
  For all local-zones types, if the DNS query matches, it is answered Authoritatively. How a non-matching query is handled depends on the local-zone **type**.
  deny drops the query.
  refuse sends a REFUSED response.
  static sends either a NoData or NXDOMAIN response (includes SOA if present in local-zone).
  transparent performs regular cache operation (i.e. transparent pass-through or iterative resolution) except for those query names which would result in NoData. This is the default local-zone **type**.
  type-transparent Same as **transparent** but does not return NoData.
  redirect returns responses with zone suffix record(s) for queries beneath that suffix. For example, a local-zone for example.com and a single A record for that name; queries for www.example.com or abc.www.example.com would return the single A record (both have the same suffix).
- **max-concurrent-queries**
  Specifies the maximum number of concurrent distinct queries used by the resolver. A query is identified by query name, type and class. If the number of distinct queries exceeds this limit, the resolver replaces the earliest query in the queue with the new query if it has been in the queue longer than the allowed time. The default value is **1024**.
- **max-concurrent-tcp**
  Specifies the maximum number of concurrent TCP flows used by the resolver. The default value is **20**.
- **max-concurrent-udp**
  Specifies the maximum number of concurrent UDP flows used by the resolver. The default value is **8192**.
- **msg-cache-size**
  Specifies the maximum size in bytes of the DNS message cache. The default value is **1048576**.
  The BIG-IP system caches the messages in a DNS response in the message cache. After the maximum size of the cache is reached, when new or refreshed content is added to the cache, the expired and older content is removed from the cache. A higher maximum size allows more DNS responses to be cached and increases the cache hit percentage. A lower maximum size forces earlier eviction of cached content, but can lower the cache hit percentage.

- **name**
  Specifies a unique name for the component. This option is required for the commands **create**, **delete**, and **modify**.
- **nameserver-cache-count**
  Specifies the maximum number of DNS nameservers for which the BIG-IP system caches connection and capability data. The default value is **16536** entries.
- **prefetch-key**
  When enabled, the validating resolver fetches the DNSKEY early in the validation process. Disable this setting when you want to reduce resolver traffic, but understand that a client may have to wait for the validating resolver to perform a key lookup. The default value is **yes**.
- **randomize-query-name-case**
  When enabled, the resolver randomizes the case of query names. The default value is **yes**.
- **regex**
  Displays the items that match the regular expression. The regular expression must be preceded by an at sign (@[regular expression]) to indicate that the identifier is a regular expression. See **help regex** for a description of regular expression syntax.
- **response-policy-zones**
  Adds, deletes or modifies the response policy zone to be used by this DNS Cache. Only a DNS Express zone configured as a response policy zone can be added.
  The query name of a recursive DNS request without DNSSEC enabled is queried against the data in the response policy zone. If a match is found, the configured response policy action is taken.
  - **action**
    The action to take upon a match. **nxdomain** results in an NXDOMAIN response given to the client. **walled-garden** results in a response with a CNAME to the walled-garden zone and an A or AAAA response matching the DNS query type. The default action is **nxdomain**.
  - **walled-garden**
    A local zone configured in this cache that contains an A and/or AAAA record. This is typically used to redirect a user that requests resolution of a name contained in the RPZ database to a local server. This local server can display a message to the user and/or record the connection. Only A/AAAA/ANY requests are redirected, a request for any other type is answered with a NoData response. If a request is received for type A or AAAA but there are no records of that type configured, a NoData response is returned instead.

- **root-hints**
  Specifies the IP addresses of DNS servers that the BIG-IP system considers authoritative for the DNS root nameservers.

Important

By default, the BIG-IP system uses the DNS root nameservers published by InterNIC.
Caution: *When you add DNS root nameservers, the BIG-IP system no longer uses the default nameservers published by InterNIC, but instead uses the nameservers you add as authoritative for the DNS root nameservers.*

- **route-domain**
  Specifies the route domain the resolver uses for outbound traffic. The default value is the default route domain.
- **rrset-cache-size**
  Specifies the maximum size in bytes of the resource records set cache. The default value is **10485760**.
  The BIG-IP system caches the supporting records in a DNS response in the resource record cache. After the maximum size of the cache is reached, when new or refreshed content is added to the cache, the expired and older content is removed from the cache. A higher maximum size allows more DNS responses to be cached and increases the cache hit percentage. A lower maximum size forces earlier eviction of cached content, but can lower the cache hit percentage.
- **trust-anchors**
  Specifies the DNSKEY or DS resource records the BIG-IP system uses to establish DNSSEC trust with a specific DNS zone. The resource records must be specified in string format, for example, dig or drill format. The default value is **none**.
- **unwanted-query-reply-threshold**
  The system always rejects unsolicited replies. The default value of **0** (off) indicates the system does not generate SNMP traps or log messages when rejecting unsolicited replies.
  Change the default value to monitor for unsolicited DNS replies. This alerts you to a potential security attack, such as cache poisoning or DOS. For example, if you specify a value of 1,000,000, each time the system receives 1,000,000 unsolicited replies, it generates an SNMP trap and log message. The default value is **0** (off).
- **use-ipv4**
  When enabled, the resolver sends DNS queries to IPv4 addresses. The default value is **yes**.
- **use-ipv6**
  When enabled, the resolver sends DNS queries to IPv6 addresses. The default value is **yes**.
- **use-tcp**
  When enabled, the resolver can send queries over the TCP protocol. The default value is **yes**.

- **use-udp**
  When enabled, the resolver can send queries over the UDP protocol. The default value is **yes**.

See Also

create, *delete*, *edit*, glob, *list*, *transparent*, *resolver*, *show*, *modify*, regex, *tmsh*

59

ltm dns cache records

- Introducing the ltm dns cache records module
- Alphabetical list of components

Introducing the ltm dns cache records module

You can use the tmsh components that reside within the ltm dns cache records module to configure DNS cache records for Local Traffic Manager™. For more information about the tmsh hierarchical structure, see Chapter 2, *Understanding and Using the Traffic Management Shell*.

Alphabetical list of components

The remainder of this chapter lists the tmsh components that are available in the ltm dns cache records module.

key

Manages the DNSKEY records in the DNS caches on the BIG-IP® system.

Syntax

Configure the **key** component within the **ltm dns cache records** module using the following syntax.

Display

```
show key cache [cache name]
    count-only
    owner [domain name]
    slot [integer]
    tmm [integer]
```

Delete

```
delete key cache [cache name]
    owner [domain name]
```

Examples

show key cache resolver_cache

Displays the DNSKEY records in the cache named **resolver_cache**.

delete key cache v_resolver_cache

Deletes the DNSKEY records from the cache named **v_resolver_cache**.

Description

You can use the following options with the **key** component.

Options

- **cache name**
  Specifies a DNS cache name from which to display or delete DNSKEY records. This is a required field.
- **count-only**
  For a show command, return only a count of the number of matched records.
- **owner**
  Specifies a domain name on which to filter the DNSKEY records in the specified DNS cache for a query or deletion.

- **slot**
  Specifies a slot number on a chassis that contains the specified DNS cache. This is a 1 based index.
- **tmm**
  Specifies the number of the TMM that contains the specified DNS cache. Use this option only for during debugging. This is a 0 based index.

See Also

delete, *show*, *tmsh*

msg

Manages message records in the DNS caches on the BIG-IP® system.

Syntax

Configure the **msg** component within the **ltm dns cache records** module using the following syntax.

Display

```
show msg cache [cache name]
    count-only
    qname [domain name]
    rcode [integer]
    slot [integer]
    tmm [integer]
```

Delete

```
delete msg cache [cache name]
    qname [domain name]
    rcode [integer]
```

Description

The **msg** component contains full DNS messages. You can display and delete these messages.

Examples

show msg cache resolver_cache

Displays the message records in the DNS cache named **resolver_cache**.

delete msg cache v_resolver_cache

Deletes the message records from the DNS cache named **v_resolver_cache**.

Options

- **cache name**
  Specifies a DNS cache name. This is a required field.
- **count-only**
  For a show command, return only a count of the number of matched records.

- **qname**
  Specifies a domain name on which to filter the DNS messages in the specified DNS cache for a query or deletion.
- **rcode**
  Specifies the DNS return code on which to filter DNS messages in the specified DNS cache for a query or deletion.
- **slot**
  Specifies a slot number on a chassis that contains the specified DNS cache. This is a 1 based index.
- **tmm**
  Specifies the number of the TMM that contains the specified DNS cache. This is a 0 based index.

See Also

delete, *show*, *tmsh*

nameserver

Manages the nameserver records in the DNS cache resolvers on the BIG-IP® system.

Syntax

Configure the **nameserver** component within the **ltm dns cache records**

Display

```
show cache [cache name]
    address [ip address]
    count-only
    has-edns [yes | no]
    has-lame [yes | no]
    rtt-range [min:max]
    slot [integer]
    tmm [integer]
    ttl-range [min:max]
    zone-name [name]
```

Delete

```
delete cache [cache name]
    address [ip address]
    has-edns [yes | no]
    has-lame [yes | no]
    rtt-range [min:max]
    ttl-range [min:max]
    zone-name [name]
```

Description

You can use the **nameserver** component to display or delete nameserver records from a DNS cache. The maximum number of records returned is 1000; therefore, broad searches may not show all records in the cache.

Examples

show cache my_cache zone-name com ttl-range 50:500

Displays the nameserver records, in the DNS cache named **my_cache**, with the zone name **com**, where the TTLs of the records are between **50** and **500**.

Options

- **address**
  Specifies the nameserver records, in the specified DNS cache, to select based on the IP address of the nameserver.
- **cache name**
  Specifies a DNS cache name. This is a required field.
- **count-only**
  For a show command, return only a count of the matched records.
- **has-edns**
  Specifies the nameserver records to select from the specified DNS cache, based on whether the nameserver is EDNS lame. An EDNS lame nameserver does not reply to EDNS queries.
- **has-lame**
  Specifies the nameserver records to select from the specified DNS cache, based on whether the nameserver is lame for one or more items.
- **rtt-range**
  Specifies the nameserver records to select from the specified DNS cache, based on RTTs within the specified range (inclusive). A missing value (:500 or 50:) defaults to the minimum or maximum, respectively.
- **slot**
  Specifies a slot number on a chassis that contains the specified DNS cache. This is a 1 based index.
- **tmm**
  Specifies the number of the TMM that contains the specified DNS cache. This is a 0 based index.
- **ttl-range**
  Specifies the nameserver records to select from the specified DNS cache, based on TTLs within the specified range (inclusive). A missing value (:500 or 50:) defaults to the minimum or maximum, respectively.
- **zone-name**
  Specifies the nameserver records to select from the specified DNS cache, based on the specified zone name.

See Also

delete, *show*, *tmsh*

rrset

Manages the RRset records in the DNS cache resolvers on the BIG-IP® system.

Syntax

Configure the **rrset** component within the **ltm dns cache records** module using the syntax in the following sections.

Display

```
show cache [cache name]
    class [IN | CH | HS| ANY]
    count-only
    owner [DNS name]
    slot [integer]
    tmm [integer]
    ttl-range [integer:integer]
    type [A | AAAA | CNAME | NS | PTR | RRSIG | DNSKEY | SOA | TXT | ANY | ... ]
```

Delete

```
delete cache [cache name]
    class [IN | CH | HS| ANY]
    owner [DNS name]
    ttl-range [integer:integer]
    type [A | AAAA | CNAME | NS | PTR | RRSIG | DNSKEY | SOA | TXT | ANY | ... ]
```

Description

You can use the **rrset** component to display or delete records in the specified DNS cache. The maximum number of records returned is **1000**. Broad searches might not show all records in the cache.

Examples

show cache resCache2 class IN type A ttl-range 20:5000 owner .com

Displays RRset records of type A, class **IN**, with TTLs between **20** and **5000**, and an owner of **.com**.

Options

- **cache name**
  Specifies a DNS cache name. This is a required field.

- **class**
  Specifies the class of RRset records to select from the specified DNS cache.
- **count-only**
  For a show command, return only a count of the matched records.
- **owner**
  Specifies the node on which to filter the RRset records in the specified DNS cache for a query or deletion.
- **slot**
  Specifies a slot number on a chassis that contains the specified DNS cache. This is a 1 based index.
- **tmm**
  Specifies the number of the TMM that contains the specified DNS cache. This is a 0 based index.
- **ttl-range**
  Specifies the RRset records to select from the specified DNS cache, based on TTLs within the specified range (inclusive). A missing value (:500 or 50:) defaults to the minimum or maximum, respectively.
- **type**
  Specifies the RRset records to select from the specified DNS cache, based on the specified type. Most record types are supported.

See Also

show, *delete*, *tmsh*

60

ltm dns dnssec

- Introducing the ltm dns dnssec module
- Alphabetical list of components

Introducing the ltm dns dnssec module

You can use the tmsh components that reside within the ltm dns dnssec module to configure components that enable DNS security extensions.

For information about the tmsh hierarchical structure, see Chapter 2, *Understanding and Using the Traffic Management Shell*.

Alphabetical list of components

The remainder of this chapter lists the tmsh components that are available in the ltm dns dnssec module.

generation

Configures a generation on the BIG-IP® system.

Syntax

Configure the **generation** component within the **ltm dns dnssec** module using the syntax in the following sections.

Create/Modify

```
modify generation [name]
    app-service [[string] | none]
    expiration [date and time]
    rollover [date and time]
edit generation [ [ [name] | [glob] | [regex] ] ... ]
   all-properties
   non-default-properties
```

Display

```
list generation
list generation [ [ [name] | [glob] | [regex] ] ... ]
    all-properties
    non-default-properties
    pub-text
show generation
show generation [ [ [name] | [glob] | [regex] ] ... ]
    (default | exa | gig | kil | meg | peta | raw | tera | yotta | zetta)
```

Delete

```
delete generation [name]
```

Description

You can use the **generation** component to configure a generation.

Examples

list generation myfirstgen

Displays the properties of the generation named **myfirstgen**.

show generation myfirstgen

Displays the status of the generation named **myfirstgen**.

Options

- **app-service**
  Specifies the name of the application service to which this generation belongs. The default value is **none**. **Note:** If the **strict-updates** option is **enabled** on the application service that owns the object, you cannot modify or delete this generation. Only the application service can modify or delete this generation.
- **expiration**
  Specifies the date and time that this generation expires.
- **glob**
  Displays the items that match the **glob** expression. See **help glob** for a description of **glob** expression syntax.
- **name**
  Specifies a unique name for the component. This option is required for the commands **create**, **delete**, and **modify**.
- **pub-text**
  Displays public text generated by the system.
- **regex**
  Displays the items that match the regular expression. The regular expression must be preceded by an at sign (@[regular expression]) to indicate that the identifier is a regular expression. See **help regex** for a description of regular expression syntax.
- **rollover**
  Specifies the date and time that this generation rolls over to a new generation.

See Also

create, *delete*, *edit*, glob, *list*, *modify*, regex, *show*, *tmsh*

key

Configures DNSSEC keys on the BIG-IP® system.

Syntax

Configure the **key** component within the **ltm dns dnssec** module using the syntax in the following sections.

Create/Modify

```
create key [name]
modify key [name]
    algorithm [ rsasha1 | rsasha256 | rsasha512 ]
    app-service [[string] | none]
    bitwidth [ 512 | 1024 | 2048 | 4096 ]
    certificate-file [string]
    description [string]
    [enabled | disabled]
    expiration-period [integer]
    key-file [string]
    key-type [ksk | zsk]
    rollover-period [integer]
    signature-pub-period [integer]
    signature-valid-period [integer]
    ttl [integer]
    use-fips [external | internal | none]
edit key [ [ [name] | [glob] | [regex] ] ... ]
   all-properties
   non-default-properties
```

Display

```
list key
list key [ [ [name] | [glob] | [regex] ] ... ]
    all-properties
    generation
    non-default-properties
    one-line
```

Delete

```
delete key [name]
```

Description

You can use the **key** component to configure DNSSEC zone signing and key signing keys, and to view information about the keys.

Examples

create key ksk1

Creates the key signing key, **ksk1**, using the system default values.

create key zsk1

Creates the zone signing key, **zsk1**, using the system default values.

list key my_key

Displays the properties of the DNS security key **my_key**.

Options

- **algorithm**
  Specifies the algorithm to use to generate the key. The default value is **RSASHA1**.
- **app-service**
  Specifies the name of the application service to which the key belongs. The default value is **none**. **Note:** If the **strict-updates** option is **enabled** on the application service that owns the object, you cannot modify or delete the key. Only the application service can modify or delete the key.
- **bitwidth**
  Specifies the length of the key you want to generate. The default value is **1024**. If a key is manually managed, MCPD will derive this value from the file and override any user defined value.
- **certificate-file**
  Specifies the file containing the public key. Fields **certificate-file** and **key-file** are required for manual DNSSEC key import.
- **description**
  User defined description.
- **[enabled | disabled]**
  Specifies whether the key is **enabled** or **disabled**.
- **expiration-period**
  Specifies the life of the key in d:h:m:s, h:m:s, m:s, or seconds. At the end of the period, the system deletes the expired generation of the key. This value must be greater than the value of the **rollover-period** option. The difference between the two periods must be more than the value of the **ttl** option.
  The default value is **0** (zero), which indicates unset, and thus the key does not expire.
- **generation**
  Displays the generation of the key, including the following:
  - **creator**
    Hostname of BIG-IP system that created this generation.
  - **expiration**
    The date and time that this generation of the key expires.

- **handle**
  The handle of a generation of a key that is used for interacting with the key subsystem (for example, HSM for FIPS).
- **key-tag**
  The hash identifier of the DNSKEY.
- **pub-text**
  The text of the randomly-generated public key.
- **rollover**
  The date and time that this generation of the key rolls over to a new key.

◆ **glob**
Displays the items that match the **glob** expression. See **help glob** for a description of **glob** expression syntax.

◆ **key-file**
Specifies the file containing the private key. Fields **certificate-file** and **key-file** are required for manual DNSSEC key import.

◆ **key-type**
Specifies whether the key is of type ksk or zsk. The default value is **zsk**.

◆ **name**
Specifies a unique name for the component. This option is required for the commands **create**, **delete**, and **modify**.

◆ **regex**
Displays the items that match the regular expression. The regular expression must be preceded by an at sign (@[regular expression]) to indicate that the identifier is a regular expression. See **help regex** for a description of regular expression syntax.

◆ **rollover-period**
Specifies the amount of time, in d:h:m:s, h:m:s, m:s, or seconds, before the system generates another generation of the key. At the end of the period, the system creates a new generation of the key. Two generations of the key exist during the time between the end of the rollover period and the end of the expiration period.
This value must be greater than or equal to one third of the value of the **expiration-period** option, and less than the value of the **expiration period** option. The difference between the two periods must be must be more than the value of the **ttl** option.
The default value is **0** (zero), which indicates unset, and thus the key does not roll over.

◆ **signature-pub-period**
Specifies the amount of time, in d:h:m:s, h:m:s, m:s, or seconds, before the system publishes another generation of the signature. At the end of the period, the system creates a new signature.
This value must be less than the value of the **signature-valid-period** option. The default value is **403200** seconds.

- **signature-valid-period**
  Specifies the amount of time, in d:h:m:s, h:m:s, m:s, or seconds, that the signature is valid. At the end of the period, the Global Traffic Manager no longer uses the expired signature. The default value is **604800** seconds.
- **ttl**
  Specifies the amount of time, in d:h:m:s, h:m:s, m:s, or seconds, that a DNS server can cache the key. The default value is **86400**.
  The value of the ttl option must be less than the difference between the values of the **rollover-period** and **expiration-period** options.
  0 seconds indicates that the key is not cached.
- **use-fips**
  Specifies the type of FIPS-compliant hardware security module to use when storing, and signing with, the private key. The default value is **none**. The choice of **external** attempts to use a network-attached FIPS device if configured; otherwise **internal** uses the FIPS device within the BIG-IP.
  If this option is set to **internal** or **external** and a FIPS device is not present, the system automatically resets the value to **none**.

See Also

create, *delete*, *edit*, glob, *list*, *modify*, regex, *tmsh*

zone

Configures DNSSEC zones on the BIG-IP® system.

Syntax

Configure the **zone** component within the **ltm dns dnssec** module using the syntax in the following sections.

Create/Modify

```
create zone [name]
modify zone [name]
    app-service [[string] | none]
    description [string]
    [enabled | disabled]
    ds-algorithm [ SHA1 | SHA256 ]
    keys
      [add | delete | modify | replace-all-with] {
        [key name ...]
    }
    keys none
    nsec3-algorithm [ SHA1 ]
    nsec3-iterations [unsigned integer]
edit zone [ [ [name] | [glob] | [regex] ] ... ]
   all-properties
   non-default-properties
reset-stats zone
reset-stats zone [ [ [name] | [glob] | [regex] ] ... ]
```

Display

```
list zone
list zone [ [ [name] | [glob] | [regex] ] ... ]
    all-properties
    non-default-properties
    one-line
    seps
show zone [ [ [name] | [glob] | [regex] ] ... ]
    (default | exa | gig | kil | meg | peta | raw | tera | yotta | zetta)
    global
    field-fmt
```

Delete

```
delete zone [name]
```

Description

You can use the **zone** component to configure and view information about a DNSSEC zone.

Examples

list zone mySecureZone

Displays the properties of the DNSSEC zone named **mySecureZone**.

Options

- **app-service**
  Specifies the name of the application service to which the zone belongs. The default value is **none**. **Note:** If the **strict-updates** option is **enabled** on the application service that owns the object, you cannot modify or delete the zone. Only the application service can modify or delete the zone.
- **description**
  User defined description.
- **ds-algorithm**
  Specifies the hash algorithm to use when creating the Delegation Signer (DS) resource record. The default value is **SHA1**.
- **[enabled | disabled]**
  Specifies whether the DNSSEC zone is **enabled** or **disabled**.

◆ Note

You must associate both a key signing and a zone signing key with the zone before complete signing of client requests can occur.

- **glob**
  Displays the items that match the **glob** expression. See **help glob** for a description of **glob** expression syntax.
- **keys**
  Specifies the keys that you want to configure for the zone.
- **name**
  Specifies a unique name for the component. This option is required for the commands **create**, **delete**, and **modify**.
- **nsec3-algorithm**
  Specifies the hash algorithm to use when creating the Next Secure (NSEC3) resource record. The default value is **SHA1**.
- **nsec3-iterations**
  Specifies the number of times to hash the Next Secure (NSEC3) names. The default value is 1."
- **regex**
  Displays the items that match the regular expression. The regular expression must be preceded by an at sign (@[regular expression]) to indicate that the identifier is a regular expression. See **help regex** for a description of regular expression syntax.

- **seps**
  Displays the Secure Entry Point(s) (DS and DNSKEY resource records used as client trust anchors) of the zone, including the following:
  - **dnskey**
    String representation of the DNSKEY resource record.
  - **ds**
    String representation of the DS resource record.
  - **generation-id**
    ID of DNSSEC Key Generation used to create the SEP.
  - **key-name**
    Name of DNSSEC Key which was used to create the SEP.
  - **xfr-primary-soa-serial**
    The learned zone SOA serial number from the primary server.
  - **xfr-soa-serial**
    The advertised zone SOA serial number to all clients.

See Also

create, *delete*, *edit*, glob, *list*, *modify*, regex, *tmsh*

61

ltm global-settings

- Introducing the ltm global-settings module
- Alphabetical list of components

Introducing the ltm global-settings module

You can use the tmsh components that reside within the ltm global-settings module to configure global settings for Local Traffic Manager™. For more information about the tmsh hierarchical structure, see Chapter 2, *Understanding and Using the Traffic Management Shell*.

Alphabetical list of components

The remainder of this chapter lists the tmsh components that are available in the ltm global-settings module.

connection

Configures the global settings that pertain to connections for the BIG-IP® and VIPRION® local traffic management systems.

Syntax

Configure the **connection** component within the **ltm global-settings** module using the syntax shown in the following sections.

Modify

```
modify connection
    adaptive-reaper-hiwater [integer]
    adaptive-reaper-lowater [integer]
    auto-last-hop [disabled | enabled]
    global-flow-eviction-policy [name]
    syncookies-threshold [integer]
    vlan-keyed-conn [disabled | enabled]
```

Display

```
list connection
list connection [option name]
show running-config connection
show running-config connection [option name]
    all-properties
    non-default-properties
    one-line
```

Description

You can use the **connection** component to modify how the system processes connections.

Examples

- **modify connection auto-last-hop disabled**
  Specifies that the system does not automatically map the last hop for pools.
- **list connection**
  Displays the global settings for how the system processes connections.

Options

- **adaptive-reaper-hiwater**
  IMPORTANT This command has been deprecated (as of 11.6.0). Please use ltm eviction-policy instead. Specifies, in a percentage, the

memory usage at which the system stops establishing new connections. Once the system meets the reaper high-water mark, the system does not establish new connections until the memory usage drops below the reaper low-water mark. The adaptive reaper settings help mitigate the effects of a denial-of-service attack.
The available range is **85 - 100**. The default value is **95**. To disable the adaptive reaper, set the high-water mark to **100**.

- **adaptive-reaper-lowater**
IMPORTANT This command has been deprecated (as of 11.6.0). Please use ltm eviction-policy instead. Specifies, in percent, the memory usage at which the system silently purges stale connections, without sending reset packets (RST) to the client. If the memory usage remains above the low-water mark after the purge, then the system starts purging established connections closest to their service timeout.
The available range is **70 - 100**. The default value is **85**. To disable the adaptive reaper, set the low-water mark to **100**.
- **auto-last-hop**
Specifies that the system automatically maps the last hop for pools. The default value is **enabled**.
- **global-flow-eviction-policy**
Specifies the flow eviction policy to use when approaching memory usage limits. The settings in the policy determine the adaptive reaper high and low water marks, and help determine which client connections to terminate when memory limits have exceeded the "low-water" threshold in the eviction policy. The settings help mitigate the effects of a denial-of-service attack.
- **syncookies-threshold**
Specifies the number of new or untrusted TCP connections that can be established before the system activates the SYN Cookies authentication method for subsequent TCP connections. The default value is **16384**.
- **vlan-keyed-conn**
Enables or disables VLAN-keyed connections. You use VLAN-keyed connections when traffic for the same connection must pass through the system several times, on multiple pairs of VLANs (or in different VLAN groups). The default value is **enabled**.

See Also

list, *node*, *modify*, *show*, *tmsh*

general

Configures the general properties for the BIG-IP® and VIPRION® local traffic management systems.

Syntax

Configure the **general** component within the **ltm global-settings** module using the syntax shown in the following sections.

Modify

```
modify general
   gratuitous-arp-rate [integer value: 0 ~ 2147483647]
   l2-cache-timeout [ integer value: 0 ~ 2147483647]
   maintenance-mode [disabled | enabled]
   share-single-mac [unique | global | vmw-compat]
   snat-packet-forward [ disabled | enabled]
```

Display

```
list general
list general [option name]
show running-config general
show running-config general [option name]
    all-properties
    non-default-properties
    one-line
```

Description

You can use the **general** component to modify how the system processes local traffic.

Examples

- **modify general maintenance-mode enabled**
  Places the Local Traffic Manager system in maintenance mode.
- **list general**
  Displays the general properties of the local traffic management system.

Options

- **gratuitous-arp-rate**
  Specifies how fast gratuitous ARPs can be sent. If it is 0, then gratuitous ARPs are sent without pause. Otherwise, it specifies how many gratuitous ARPs can be sent every second. The default value is 0. The range is **0** (zero) to **2147483647**."
- **l2-cache-timeout**
  Specifies, in seconds, the amount of time that records remain in the Layer 2 forwarding table, when the MAC address of the record is no longer detected on the network.
  The default value is **300** seconds. The range is **0** (zero) to **2147483647** seconds.
- **maintenance-mode**
  Specifies, when enabled, that the unit is in maintenance mode. In maintenance mode, the system stops accepting new connections and slowly finishes off existing connections.
  The default value is **disabled**.
- **share-single-mac**
  Specifies the Media Access Control address (MAC address) that the system assigns to a VLAN. The default value is **unique**, which indicates that a VLAN uses a unique MAC address from the pool of mac addresses assigned to each hardware platform. The **global** value indicates that all of the VLANs on the system use the same MAC address. The **vmw-compat** value indicates that the MAC address of a vlan is allocated in a manner compatible with VMware™ vSwitch, and restricts vlans to a single interface, with no trunks allowed. Changing the value of this feature requires a manual restart of all TMOS daemons.
- **snat-packet-forward**
  Enables or disables SNAT packet forwarding. The default value is **enabled**.

See Also

list, *node*, *modify*, *show*, *tmsh*

traffic-control

Configures the global settings that pertain to traffic control for the BIG-IP® and VIPRION® local traffic management systems.

Syntax

Configure the **traffic-control** component within the **ltm global-settings** module using the syntax shown in the following sections.

Modify

```
modify traffic-control
    accept-ip-options [disabled | enabled]
    accept-ip-source-route [disabled | enabled]
    allow-ip-source-route [ disabled | enabled]
    continue-matching [ disabled | enabled]
    max-icmp-rate [integer value: 0 ~ 2147483647]
    max-reject-rate [ integer value: 1 ~ 1000]
    min-path-mtu [ integer value: 68 ~ 1500]
    path-mtu-discovery [disabled | enabled]
    port-find-linear [ integer value: 0 ~ 61439]
    port-find-random [ integer value: 0 ~ 1024]
    reject-unmatched [ disabled | enabled]
```

Display

```
list traffic-control
list traffic-control [option name]
show running-config traffic-control
show running-config traffic-control [option name]
    all-properties
    non-default-properties
    one-line
```

Description

You can use the **traffic-control** component to modify how the system processes local traffic.

Examples

- **modify traffic-control accept-ip-options enabled**
  Specifies that the system accepts IPv4 packets with IP options.
- **list traffic-control**
  Displays the local traffic control global settings.

Options

- **accept-ip-options**
  Specifies whether the system accepts IPv4 packets with IP options. The default value is **disabled**.
- **accept-ip-source-route**
  Specifies whether the system accepts IPv4 packets with IP source route options that are destined for Traffic Management Microkernel (TMM). The default value is **disabled**.
  To enable this option, you must also enable the **accept-ip-options** option.
- **allow-ip-source-route**
  Specifies whether the system allows IPv4 packets with IP source route options enabled to be routed through Traffic Management Microkernel (TMM). The default value is **disabled**.
  To enable this option, you must also enable the **accept-ip-options** option.
- **continue-matching**
  Specifies whether the system matches against a less-specific virtual server when the more-specific one is disabled. When **continue-matching** is **disabled**, the default value, the system drops connections that request a disabled virtual server. In this case, the system rejects or drops packets depending on the value of the **reject-unmatched** option.
- **max-icmp-rate**
  Specifies the maximum rate per second at which the system issues Internet Control Message Protocol (ICMP) errors. The default value is **100** errors per second. The range is from **0** (zero) to **2147483647** errors per second. This option is useful for preventing ICMP-message storms.
- **max-reject-rate**
  Specifies the maximum rate per second at which the system issues reject packets (TCP RST or ICMP port unreach). The default value is **250** per second. The range is from **1** to **1000** per second.
- **min-path-mtu**
  Specifies the minimum packet size that can traverse the path without suffering fragmentation, also known as path Maximum Transmission Unit(MTU). The default value is **296**. The range is from **68** to **1500**.
- **path-mtu-discovery**
  Specifies, when enabled, that the system discovers the maximum transmission unit (MTU) that it can send over a path, without fragmenting TCP packets. The default value is **enabled**.
- **port-find-linear**
  Specifies the maximum of ports to linearly search for outbound connections. The default value is **16**. The range is from **0** to **61439**.
- **port-find-random**
  Specifies the maximum of ports to randomly search for outbound connections. The default value is **16**. The range is from **0** to **1024**.

- **reject-unmatched**
  Specifies, when enabled, that the system returns a TCP RESET or ICMP_UNREACH packet if no virtual servers on the system match the destination address of the incoming packet. When this option is disabled, the system silently drops the unmatched packet. The default value is **enabled**.

See Also

list, *node*, *modify*, *show*, *tmsh*

62

ltm message-routing generic

- Introducing the ltm message-routing generic module
- Alphabetical list of components

Introducing the ltm message-routing generic module

You can use the tmsh components that reside within the LTM Message-Routing Generic module to configure generic messaging between two or more BIG-IP systems. For more information about the tmsh hierarchical structure, see Chapter 2, *Understanding and Using the Traffic Management Shell*.

Alphabetical list of components

The remainder of this chapter lists the tmsh components that are available in the ltm message-routing generic module.

peer

Configures a peer for routing generic message protocol messages.

Syntax

Configure the **peer** component within the **ltm message-routing generic** module using the syntax shown in the following sections.

Create/Modify

```
create peer [name]
modify peer [name]
    connection-mode [ per-peer | per-blade | per-tmm ]
    number-connections [integer]
    pool [name]
    ratio [integer]
    transport-config [ transport-config ]
edit peer [ [ [name] | [glob] | [regex] ] ... ]
    all-properties
    non-default-properties
reset-stats peer
reset-stats peer [ [ [name] | [glob] | [regex] ] ... ]
```

Display

```
list peer
list peer [ [ [name] | [glob] | [regex] ] ... ]
show running-config peer
show running-config peer [ [ [name] | [glob] | [regex] ] ... ]
    all-properties
    non-default-properties
    one-line
    partition
show peer
show peer [ [ [name] | [glob] | [regex] ] ... ]
    (default | exa | gig | kil | meg | peta | raw | tera | yotta | zetta)
    field-fmt
```

Delete

```
delete peer [name]
```

Description

You can use the **peer** component to manage a named generic message peer. A peer specifies the pool for the generic message parser to use as the destination for generic message routes. You can also use the **peer** component to specify how many connections the parser creates to a remote host and what transport the parser uses to establish the connection.

Examples

create peer my_peer { pool my_pool transport { type virtual name my_vip } }

Creates a generic message peer named **my_peer** which uses the settings of **my_vip** to establish a connection with a pool member from pool **my_pool**.

- **connection-mode**
  Specifies how the number of connections per host are limited. Note a host (specified in the referred pool) may exist more than one peer object, and those peer objects may have different settings for **connection-mode** and **number_connections**. Thus, these settings specify how messages routed through this peer are distributed between a set of connections, not the maximum number of connections to a specified host. The default value is **per-peer**.
  - **per-peer**
    Specifies the number of connections to a remote host.
  - **per-blade**
    Specifies the number of connections to a remote host per blade in the cluster.
  - **per-tmm**
    Specifies the number of connections to a remote host per TMM in the system.
- **number-connections**
  Specifies the distribution of connections between the BIG-IP system and a remote host. The default value is **1**.
- **pool**
  Specifies the name of the pool to which the generic parser routes messages.
- **ratio**
  Specifies the ratio the generic message parser uses to select a **peer** from a list of peers for the **ltm message-routing generic route**. The default value is **1**.
- **transport-config**
  Specifies the name of the transport configuration (ltm message-routing generic transport-config) the message router uses to create an outgoing connection.

See Also

create, *delete*, *edit*, glob, *list*, *virtual*, *modify*, regex, *reset-stats*, *show*, *tmsh*, *route protocol*

protocol

Configures a generic message protocol component for parsing generic messages.

Syntax

Configure the **protocol** component within the **ltm message-routing generic** module using the syntax shown in the following sections.

Create/Modify

```
create protocol [name]
modify protocol [name]
    defaults-from [ [name] | none]
    disable-parser [ yes | no ]
    max-egress-buffer [integer]
    max-message-size [integer]
    message-terminator [string]
    no-response [ yes | no ]
edit protocol [ [ [name] | [glob] | [regex] ] ... ]
    all-properties
    non-default-properties
reset-stats protocol
reset-stats protocol [ [ [name] | [glob] | [regex] ] ... ]
```

Display

```
list protocol
list protocol [ [ [name] | [glob] | [regex] ] ... ]
show running-config protocol
show running-config protocol [ [ [name] | [glob] | [regex] ] ... ]
    all-properties
    non-default-properties
    one-line
    partition
show protocol
show protocol [ [ [name] | [glob] | [regex] ] ... ]
    (default | exa | gig | kil | meg | peta | raw | tera | yotta | zetta)
    field-fmt
```

Delete

```
delete protocol [name]
```

Description

You can use the **protocol** component to implement a named generic message parser for use with the message routing framework. You can create a **protocol** component, and then add it to a virtual server. You do this when

you want to separate a stream of bytes, from a connection to a peer, into messages for routing. This also enables a set of iRule commands to create, populate, and route messages.

Examples

create protocol my_protocol defaults-from genericmsg

Creates a message protocol component named **my_protocol** using the system defaults.

create protocol my_protocol { welcome-message hello }

Creates a protocol instance named **my_protocol** that sends a welcome message of "hello" to any new connection.

- **defaults-from**
  Specifies the protocol that you want to use as the parent protocol. The new protocol inherits all of the settings and values from the specified parent protocol. The default value is **genericmsg**.
- **disable-parser**
  When set to **yes**, the generic message parser is disabled. The parser ignores all incoming packets and does not directly send message data. This mode supports iRule script protocol implementations that generate messages from the incoming transport stream and send messages on the outgoing transport stream.
- **max-egress-buffer**
  Specifies the maximum size of the send buffer in bytes. If the number of bytes in the send buffer for a connection exceeds this value, the generic message parser stops receiving outgoing messages from the router until the size of the buffer drops below this setting. The default value is **32768**.
- **max-message-size**
  Specifies the maximum size of a received message. If a message exceeds this size, the connection is reset. The default value is **32768**.
- **message-terminator**
  Specifies the string of characters used to terminate a message. If the **message-terminator** parameter is empty, the generic message parser does not separate the input stream into messages. The default value is

- **no-response**
  When set to **yes**, matching of responses to requests is disabled. The default value is **no**.

See Also

create, *delete*, *edit*, glob, *list*, *virtual*, *modify*, regex, *reset-stats*, *show*, *tmsh*, *route protocol*

route

Configures a static route the generic message parser uses to route generic message protocol messages.

Syntax

Configure the **route** component within the **ltm message-routing generic** module using the syntax shown in the following sections.

Create/Modify

```
create route [name]
modify route [name]
    destination-address [string]
    peer-selection-mode [ sequential | ratio ]
    peers { [peer-name] }
    source-address [string]
edit route [ [ [name] | [glob] | [regex] ] ... ]
    all-properties
    non-default-properties
reset-stats route
reset-stats route [ [ [name] | [glob] | [regex] ] ... ]
```

Display

```
list route
list route [ [ [name] | [glob] | [regex] ] ... ]
show running-config route
show running-config route [ [ [name] | [glob] | [regex] ] ... ]
    all-properties
    non-default-properties
    one-line
    partition
show route
show route [ [ [name] | [glob] | [regex] ] ... ]
    (default | exa | gig | kil | meg | peta | raw | tera | yotta | zetta)
    field-fmt
```

Delete

```
delete route [name]
```

Description

You can use the **route** component to manage a generic message static route.

Examples

create route my_route

Creates a static route named **my_route** that uses a wildcard value for the **source-address** and **destination-address** parameters. This acts as a default route.

create route my_route { destination-address helpdesk peers add { peer1 peer2 }

Creates a static route named **my_route** that contains two peers, **peer1** and **peer2**. Messages routed with a destination-address of **helpdesk** are routed to a pool member contained in **peer1** or **peer2**, based on the specified **peer-selection-mode**.

- **destination-address**
  Specifies the destination address of the route. If this parameter is not present, the generic message parser considers the **destination-address** as a wildcard that matches all message destination addresses. The default value is **none**.
- **peer-selection-mode**
  Specifies the method the generic message parser uses to select a peer from the specified list of peers. The default value is **sequential**.
  - **sequential**
    Specifies that the generic message parser selects the first peer in the list of peers. If the protocol retransmits the message, the generic message parser uses another pool member in the first peer. If all pool members in a peer are unavailable, the generic message parser uses the next peer in the list.
  - **ratio**
    Specifies that the generic message parser selects a peer from a list of peers based on the relative ratio values of each peer. For example if three peers have ratios of **1**, **1**, and **2**, the first 2 peers have a 25% (1/4) probability of being selected and the third peer has a 50% (2/4) probability of being selected.
- **peers**
  Specifies a list of peers.
- **source-address**
  Specifies the source address of the route. If this parameter is not present, the generic message parser considers the **source-address** as a wildcard that matches all message sources addresses. The default value is **none**.

See Also

create, *delete*, *edit*, glob, *list*, *virtual*, *modify*, regex, *reset-stats*, *show*, *tmsh*, *peer router*

router

Configures a message router instance for routing generic message protocol messages.

Syntax

Configure the **router** component within the **ltm message-routing generic** module using the syntax shown in the following sections.

Create/Modify

```
create router [name]
modify router [name]
    defaults-from [ [name] | none]
    ignore-client-port [ yes | no ]
    inherited-traffic-group [ yes | no ]
    max-pending-bytes [integer]
    max-pending-messages [integer]
    protocol [ generic-message ]
    routes { [route-name] }
    traffic-group [ [name] | none]
    use-local-connection [ yes | no ]
edit router [ [ [name] | [glob] | [regex] ] ... ]
    all-properties
    non-default-properties
reset-stats router
reset-stats router [ [ [name] | [glob] | [regex] ] ... ]
```

Display

```
list router
list router [ [ [name] | [glob] | [regex] ] ... ]
show running-config router
show running-config router [ [ [name] | [glob] | [regex] ] ... ]
    all-properties
    non-default-properties
    one-line
    partition
show router
show router [ [ [name] | [glob] | [regex] ] ... ]
    (default | exa | gig | kil | meg | peta | raw | tera | yotta | zetta)
    field-fmt
```

Delete

```
delete router [name]
```

Description

You can use the **router** component to manage a generic message router instance. All virtual servers containing the same **router** instance share the same route table and can route messages between peers.

Examples

create router my_router defaults-from messagerouter

Creates a message router instance named **my_router** using the system defaults.

create router my_router { routes add { route1 route2 } }

Creates a router instance named **my_router** that contains two static routes, **route1** and **route2**.

- **defaults-from**
  Specifies the profile that you want to use as the parent profile. The new profile inherits all of the settings and values from the specified parent profile. The default value is **messagerouter**.
- **ignore-client-port**
  If set to **yes**, the system ignores the remote port on clientside connections (connections where the peer connected to the BIG IP system) when searching for an existing connection. The default value is **no**.
- **inherited-traffic-group**
  Specifies whether the **traffic-group** is inherited from the parent folder. This value is read-only.
- **max-pending-bytes**
  Specifies the maximum number of bytes of pending messages that the router instance holds while waiting for a connection to a peer to be created. Once reached, any additional messages to the peer are flagged as undeliverable and returned to the originator. The default value is **32768**.
- **max-pending-messages**
  Specifies the maximum number of pending messages that the router instance holds while waiting for a connection to a peer to be created. Once reached, any additional messages to the peer are flagged as undeliverable and returned to the originator. The default value is **64**.
- **protocol**
  Specifies the type of message protocol this router instance uses. The default value is **generic-message**.
  The options are:
  - **generic**
    Specifies the router instance routes generic protocol messages. All virtual servers containing this router instance must also contain an LTM message routing generic protocol (ltm message-routing generic protocol).
- **routes**
  Specifies a list of static routes for the router instance to use.

- **use-local-connection**
  If set to **yes**, the router instance routes a message to an existing connection on the same TMM as the message was received. If an existing connection is not found, the router instance routes the message through an existing connection, based on a deterministic algorithm that may be on another TMM. If a matching existing connection is not found, the router instance creates a connection on the current TMM. Note that setting this parameter to **yes** may limit the number of connections the router instance can create to a peer. The default value is **yes**.

See Also

create, *delete*, *edit*, glob, *list*, *virtual*, *modify*, regex, *reset-stats*, *show*, *tmsh*, *route protocol*

transport-config

Configures a message transport-config instance for routing generic message protocol messages.

Syntax

Configure the **transport-config** component within the **ltm message-routing generic** module using the syntax shown in the following sections.

Create/Modify

```
create transport-config [name]
modify transport-config [name]
    ip-protocol [any | [protocol] ]
    source-port [integer]
    profiles [add | delete | replace-all-with] {
      [profile_name ...] {
        context [all | clientside | serverside]
      }
    }
    rules { [none | [rule_name ... ] }
    source-address-translation {
        pool [ [pool_name] | none]
        type [ automap | snat | none ]
    }
edit transport-config [ [ [name] | [glob] | [regex] ] ... ]
    all-properties
    non-default-properties
reset-stats transport-config
reset-stats transport-config [ [ [name] | [glob] | [regex] ] ... ]
```

Display

```
list transport-config
list transport-config [ [ [name] | [glob] | [regex] ] ... ]
show running-config transport-config
show running-config transport-config [ [ [name] | [glob] | [regex] ] ... ]
    all-properties
    non-default-properties
    one-line
    partition
show transport-config
show transport-config [ [ [name] | [glob] | [regex] ] ... ]
    (default | exa | gig | kil | meg | peta | raw | tera | yotta | zetta)
    field-fmt
```

Delete

```
delete transport-config [name]
```

Description

You can use the **transport-config** component to define the profiles, rules, and source-address-translation of an outgoing connection.

Examples

create transport-config my_transport-config

Creates a transport-config instance named **my_transport-config** using the system defaults.

create transport-config my_transport-config { profiles add { my_genericmsg my_tcp } }

Creates a transport-config instance named **my_transport-config** that will use two profiles, **my_genericmsg** and **my_tcp**, to create and configure an outgoing connection. The outgoing connection is automatically configured with the router instance that created the connection.

- **source-port**
  Specifies the source port to be used for the connection being created. If no value is specified an ephemeral port is chosen. The default value is **0**.
- **profiles**
  Specifies a list of profiles that the outgoing connection uses to use to direct and manage traffic. The default value is **none**.
- **rules**
  Specifies a list of iRules, separated by spaces, that customize the transport configuration to direct and manage traffic. The default value is **none**.
- **source-address-translation**
  Specifies the type of source address translation enabled for the transport configuration, as well as the pool that the source address translation uses.
  - **pool**
    Specifies the name of a SNAT pool used by the specified transport configuration.
  - **type**
    Specifies the type of source address translation associated with the specified transport configuration.
    The options are:
    - **automap**
      Specifies the use of self IP addresses for transport configuration server source address translation.
    - **none**
      Specifies no source address translation is used by the transport configuration.
    - **snat**
      Specifies the use of a SNAT pool of translation addresses for virtual server source address translation.

See Also

create, *delete*, *edit*, glob, *list*, *virtual*, *modify*, regex, *reset-stats*, *show*, *tmsh*, *route protocol*

63

ltm message-routing sip

- Introducing the ltm message-routing sip module
- Alphabetical list of components

Introducing the ltm message-routing sip module

You can use the tmsh components that reside within the LTM Message-Routing SIP module to configure generic messaging between two or more BIG-IP systems. For more information about the tmsh hierarchical structure, see Chapter 2, *Understanding and Using the Traffic Management Shell*.

Alphabetical list of components

The remainder of this chapter lists the tmsh components that are available in the ltm message-routing SIP module.

peer

Configures a peer for routing sip message protocol messages.

Syntax

Configure the **peer** component within the **ltm message-routing sip** module using the syntax shown in the following sections.

Create/Modify

```
create peer [name]
modify peer [name]
    connection-mode [ per-peer | per-blade | per-tmm ]
    number-connections [integer]
    pool [name]
    ratio [integer]
    transport-config [ transport-config ]
edit peer [ [ [name] | [glob] | [regex] ] ... ]
    all-properties
    non-default-properties
reset-stats peer
reset-stats peer [ [ [name] | [glob] | [regex] ] ... ]
```

Display

```
list peer
list peer [ [ [name] | [glob] | [regex] ] ... ]
show running-config peer
show running-config peer [ [ [name] | [glob] | [regex] ] ... ]
    all-properties
    non-default-properties
    one-line
    partition
show peer
show peer [ [ [name] | [glob] | [regex] ] ... ]
    (default | exa | gig | kil | meg | peta | raw | tera | yotta | zetta)
    field-fmt
```

Delete

```
delete peer [name]
```

Description

You can use the **peer** component to manage a named sip peer. A peer specifies the pool for the sip router to use as the destination for sip routes. You can also use the **peer** component to specify how many connections the parser creates to a remote host and what transport the parser uses to establish the connection.

Examples

create peer my_peer { pool my_pool transport { type virtual name my_vip } }

Creates a sip peer named **my_peer** which uses the settings of **my_vip** to establish a connection with a pool member from pool **my_pool**.

- **connection-mode**
  Specifies how the number of connections per host are limited. Note a host (specified in the referred pool) may exist more than one peer object, and those peer objects may have different settings for **connection-mode** and **number_connections**. Thus, these settings specify how messages routed through this peer are distributed between a set of connections, not the maximum number of connections to a specified host. The default value is **per-peer**.
  - **per-peer**
    Specifies the number of connections to a remote host.
  - **per-blade**
    Specifies the number of connections to a remote host per blade in the cluster.
  - **per-tmm**
    Specifies the number of connections to a remote host per TMM in the system.
- **number-connections**
  Specifies the distribution of connections between the BIG-IP system and a remote host. The default value is **1**.
- **pool**
  Specifies the name of the pool to which the sip parser routes messages.
- **ratio**
  Specifies the ratio the sip router uses to select a **peer** from a list of peers for the **ltm message-routing sip route**. The default value is **1**.
- **transport-config**
  Specifies the name of the transport configuration (ltm message-routing sip transport-config) the message router uses to create an outgoing connection.

See Also

create, *delete*, *edit*, glob, *list*, *virtual*, *modify*, regex, *reset-stats*, *show*, *tmsh*, *route session*

route

Configures a static route for use in Session Initiation Protocol (SIP) message routing.

Syntax

Configure the **route** component within the **ltm message-routing sip** module using the syntax shown in the following sections.

Create/Modify

```
create route [name]
modify route [name]
    app-service [[string] | none]
    from-uri [string]
    peer-selection-mode [ratio | sequential]
    peers { [none | [peer_name ... ] }
    request-uri [string]
    to-uri [string]
    virtual-server [virtual-server_name]
edit route [ [ [name] | [glob] | [regex] ] ... ]
    all-properties
    non-default-properties
```

Display

```
list route
list route [ [ [name] | [glob] | [regex] ] ... ]
show running-config route
show running-config route [ [ [name] | [glob] | [regex] ] ... ]
    all-properties
    non-default-properties
    one-line
    partition
show route
show route [ [ [name] | [glob] | [regex] ] ... ]
    (default | exa | gig | kil | meg | peta | raw | tera | yotta | zetta)
    field-fmt
```

Delete

```
delete route [name]
```

Description

You can use the **route** component to define the URI's, virtual server, peers and peer selection mode of a message routing SIP static route.

Examples

create route my_route

Creates a route instance named **my_route** using the system defaults.

create route my_route peers { peer1 peer2 }

Creates a route instance named **my_route** that will use two peers for forwarding messages.

- **app-service**
  Specifies the name of the application service to which the object belongs. The default value is **none**. **Note:** If the **strict-updates** option is **enabled** on the application service that owns the object, you cannot modify or delete the object. Only the application service can modify or delete the object.
- **from-uri**
  Specifies the patterns to be matched against the From field of a SIP message. This URI will be matched as a case insignificant method. It should be in the form of user@domain. The "sip:" prefix should not be present. Any additional modifiers (for example port or transport) should also not be present. It may begin with a wildcard, "*". If empty, it will be treated as if the entire URI was a wildcard (matching all From-URIs).
- **peer-selection-mode**
  Specifies the mode of selecting a peer from a list of peers. The options are:
  - **ratio**
    Peers are selected based on their weights in comparison with other peers.
  - **sequential**
    Peers are selected in the order listed. All traffic will route the first peer unless all pool members in the peer are marked down.
- **peers**
  Specifies an ordered list of peers to use for forwarding messages.
- **request-uri**
  Specifies the patterns to be matched against the request-uri field of a SIP message. This URI will be matched as a case insensitive method. It should be in the form of user@domain. The "sip:" prefix should not be present. Any additional modifiers (for example port or transport) should also not be present. It may begin with a wildcard, * "*". If empty, it will be treated as if the entire URI was a * wildcard (matching all Request-URIs).
- **to-uri**
  Specifies the patterns to be matched against the To field of a SIP message. This URI will be matched as a case insensitive method. It should be in the form of user@domain. The "sip:" prefix should not be present. Any additional modifiers (for example port or transport) should also not be present. It may begin with a wildcard, "*". If empty, it will be treated as if the entire URI was a wildcard (matching all To-URIs).

- **virtual-server**
  Specifies the virtual server on which connections will be routed to this route. If the virtual server is unset, messages originating on any connection may be routed to the route.

See Also

create, *delete*, *edit*, glob, *list*, *virtual*, *modify*, regex, *show*, *tmsh*, *route*

transport-config

Configures a sip transport-config instance for routing sip message protocol messages.

Syntax

Configure the **transport-config** component within the **ltm message-routing sip** module using the syntax shown in the following sections.

Create/Modify

```
create transport-config [name]
modify transport-config [name]
    ip-protocol [any | [protocol] ]
    source-port [integer]
    profiles [add | delete | replace-all-with] {
      [profile_name ...] {
        context [all | clientside | serverside]
      }
    }
    rules { [none | [rule_name ... ] }
    source-address-translation {
        pool [ [pool_name] | none]
        type [ automap | snat | none ]
    }
edit transport-config [ [ [name] | [glob] | [regex] ] ... ]
    all-properties
    non-default-properties
reset-stats transport-config
reset-stats transport-config [ [ [name] | [glob] | [regex] ] ... ]
```

Display

```
list transport-config
list transport-config [ [ [name] | [glob] | [regex] ] ... ]
show running-config transport-config
show running-config transport-config [ [ [name] | [glob] | [regex] ] ... ]
    all-properties
    non-default-properties
    one-line
    partition
show transport-config
show transport-config [ [ [name] | [glob] | [regex] ] ... ]
    (default | exa | gig | kil | meg | peta | raw | tera | yotta | zetta)
    field-fmt
```

Delete

```
delete transport-config [name]
```

Description

You can use the **transport-config** component to define the profiles, rules, and source-address-translation of an outgoing connection.

Examples

create transport-config my_transport-config

Creates a transport-config instance named **my_transport-config** using the system defaults.

create transport-config my_transport-config { profiles add { my_sipmsg my_tcp } }

Creates a transport-config instance named **my_transport-config** that will use two profiles, **my_sipmsg** and **my_tcp**, to create and configure an outgoing connection. The outgoing connection is automatically configured with the router instance that created the connection.

- **source-port**
  Specifies the source port to be used for the connection being created. If no value is specified an ephemeral port is chosen. The default value is **0**.
- **profiles**
  Specifies a list of profiles that the outgoing connection uses to use to direct and manage traffic. The default value is **none**.
- **rules**
  Specifies a list of iRules, separated by spaces, that customize the transport configuration to direct and manage traffic. The default value is **none**.
- **source-address-translation**
  Specifies the type of source address translation enabled for the transport configuration, as well as the pool that the source address translation uses.
  - **pool**
    Specifies the name of a SNAT pool used by the specified transport configuration.
  - **type**
    Specifies the type of source address translation associated with the specified transport configuration.
    The options are:
    - **automap**
      Specifies the use of self IP addresses for transport configuration server source address translation.
    - **none**
      Specifies no source address translation is used by the transport configuration.
    - **snat**
      Specifies the use of a SNAT pool of translation addresses for virtual server source address translation.

See Also

create, *delete*, *edit*, glob, *list*, *virtual*, *modify*, regex, *reset-stats*, *show*, *tmsh*, *route session*

64

ltm message-routing sip profile

- Introducing the ltm message-routing sip profile module
- Alphabetical list of components

Introducing the ltm message-routing sip profile module

You can use the tmsh components that reside within the LTM Message-Routing SIP profile module to configure generic messaging between two or more BIG-IP systems. For more information about the tmsh hierarchical structure, see Chapter 2, *Understanding and Using the Traffic Management Shell*.

Alphabetical list of components

The remainder of this chapter lists the tmsh components that are available in the ltm message-routing SIP profile module.

router

Configures a Session Initiation Protocol (SIP) Router profile.

Syntax

Configure the **router** component within the **ltm message-routing sip profile** module using the syntax shown in the following sections.

Create/Modify

```
create router [name]
modify router [name]
    app-service [[string] | none]
    defaults-from [[name] | none]
    max-pending-bytes [integer]
    max-pending-messages [integer]
    operation-mode [load-balancing]
    routes [add | default | delete | none | replace-all-with] {
      [route_name] ...
    }
    session {
      transaction-timeout [integer]
    }
    use-local-connection [disabled | enabled]
edit router [ [ [name] | [glob] | [regex] ] ... ]
    all-properties
    non-default-properties
reset-stats router
reset-stats router [ [ [name] | [glob] | [regex] ] ... ]
```

Display

```
list router
list router [ [ [name] | [glob] | [regex] ] ... ]
show running-config router
show running-config router [ [ [name] | [glob] | [regex] ] ... ]
    all-properties
    non-default-properties
    one-line
    partition
show router
show router [ [ [name] | [glob] | [regex] ] ... ]
    (default | exa | gig | kil | meg | peta | raw | tera | yotta | zetta)
    field-fmt
```

Delete

```
delete router [name]
```

Description

You can use the **router** component to manage a SIP router profile.

Examples

create router my_router_profile defaults-from router

Creates a SIP router profile named **my_router_profile** using the system defaults.

create router my_router_profile routes add { route1 route2 }

Creates a SIP profile named **my_router_profile** with two static routes.

Options

- **app-service**
  Specifies the name of the application service to which the object belongs. The default value is **none**. **Note:** If the **strict-updates** option is **enabled** on the application service that owns the object, you cannot modify or delete the object. Only the application service can modify or delete the object.
- **defaults-from**
  Specifies the profile that you want to use as the parent profile. Your new profile inherits all of the settings and values from the specified parent profile. The default value is **router**.
- **glob**
  Displays the items that match the **glob** expression. See **help glob** for a description of **glob** expression syntax.
- **max-pending-bytes**
  Specifies the maximum number of bytes contained within pending messages that will be held while waiting for a connection to a peer to be created. Once reached any additional messages to the peer will be flagged as undeliverable and returned to the originator.
- **max-pending-messages**
  Specifies the maximum number of pending messages that will be held while waiting for a connection to a peer to be created. Once reached any additional messages to the peer will be flagged as undeliverable and returned to the originator.
- **operation-mode**
  Specifies the behavior of the routing instance. The options are:
  - **load-balancing**
    Messages will be load balanced.
- **partition**
  Displays the administrative partition within which the component resides.

- **regex**
  Displays the items that match the regular expression. The regular expression must be preceded by an at sign (@[regular expression]) to indicate that the identifier is a regular expression. See **help regex** for a description of regular expression syntax.
- **routes**
  Specifies a list of static routes. The ordering of the route entries is insignificant.
- **session.transaction-timeout**
  Specifies the maximum time (in seconds) between a request and its response. A provisional response restarts the timer. This may not affect all transactions. The scenarios where the system waits for response (eg. a final response for REGISTER request), are impacted by dropping any persistent data maintained for the request.
- **use-local-connection**
  Enables or disables a preference for local connections established by the ingress TMM over connections established by other TMM's when selecting the egress connection to destination peer.

See Also

create, *delete*, *edit*, glob, *list*, *virtual*, *modify*, regex, *reset-stats*, *show*, *tmsh*

session

Configures a Session Initiation Protocol (SIP) Session profile.

Syntax

Configure the **session** component within the **ltm message-routing sip profile** module using the syntax shown in the following sections.

Create/Modify

```
create session [name]
modify session [name]
    app-service [[string] | none]
    custom-via [[via-header] | none]
    defaults-from [[name] | none]
    description [string]
    do-not-connect-back [disabled | enabled]
    generate-response-on-failure [disabled | enabled]
    honor-via [disabled | enabled]
    insert-record-route-header [disabled | enabled]
    insert-via-header [disabled | enabled]
    loop-detection [disabled | enabled]
    max-forwards-check [disabled | enabled]
    max-msg-header-count [integer]
    max-msg-header-size [integer]
    max-msg-size [integer]
    persistence {
      persist-key [Call-ID | Custom | Src-Addr]
      persist-timeout [integer]
      persist-type [session | none]
    }
    enable-sip-firewall [no | yes]
edit session [ [ [name] | [glob] | [regex] ] ... ]
    all-properties
    non-default-properties
reset-stats session
reset-stats session [ [ [name] | [glob] | [regex] ] ... ]
```

Display

```
list session
list session [ [ [name] | [glob] | [regex] ] ... ]
show running-config session
show running-config session [ [ [name] | [glob] | [regex] ] ... ]
    all-properties
    non-default-properties
    one-line
    partition
show session
show session [ [ [name] | [glob] | [regex] ] ... ]
    (default | exa | gig | kil | meg | peta | raw | tera | yotta | zetta)
    field-fmt
```

Delete

```
delete session [name]
```

Description

You can use the **session** component to manage a SIP session profile.

Examples

create session my_session_profile defaults-from session

Creates a SIP session profile named **my_session_profile** using the system defaults.

create session my_session_profile { insert-record-route-header enabled }

Creates a SIP profile named **my_session_profile** with insertion of record-route header in requests which establish a dialog.

Options

- **app-service**
  Specifies the name of the application service to which the object belongs. The default value is **none**. **Note:** If the **strict-updates** option is **enabled** on the application service that owns the object, you cannot modify or delete the object. Only the application service can modify or delete the object.
- **custom-via**Specifies the value the system uses for the **Sent-by** field of the Via header when the **Insert Via Header** setting is **enabled**.
  Note: The value that you enter must include a format of SIP/SIP-version/protocol, followed by a **Sent-By** value. For example, **SIP/2.0/TCP www.siterequest.com:4343** or **SIP/2.0/SCTP 10.10.4.32**.
- **defaults-from**
  Specifies the profile that you want to use as the parent profile. Your new profile inherits all of the settings and values from the specified parent profile. The default value is **session**.
- **description**
  User defined description.
- **do-not-connect-back**
  Enables or disables whether a connection to a request originator is re-established (if it no longer exists) in order to deliver a response. When disabled, responses that cannot be forwarded using an existing connection are dropped.

- **generate-response-on-failure**
  Enables or disables sending failure response messages such as 4xx, 5xx and 6xx, when a SIP request is being dropped. Note: Where it is specified "silently" discarded/dropped, no error response is generated. In any case, a dropped message (request/response) is tracked by the Messages Dropped Statistic.
- **glob**
  Displays the items that match the **glob** expression. See **help glob** for a description of **glob** expression syntax.
- **honor-via**
  Enables or disables honoring any via which is not inserted by the system for routing the response.
- **insert-record-route-header**
  Enables or disables the insertion of a record-route header in requests that establish dialog. When enabled, along with the URI, the custom parameters may be added to facilitate the routing of subsequent requests within this call to avoid route lookup. The record route URI is the local-IP and port of flows that are used for forwarding the message.
- **insert-via-header**
  Enables or disables insertion of top via. When enabled, custom parameters to help route the response back are inserted, along with sent-by field of via. The source address:port of the flow forwarding the request is filled as value for sent-by field of the via unless a custom via value is specified. The custom parameters inserted to help routing, helps improve performance as it facilitates routing without any lookup. The via is inserted at egress side of the flow, after the SIP_REQUEST_SEND event.
- **loop-detection**
  Enables or disables loop-detection checking. When a loop is detected, the request is discarded. An error response is sent, if configured. A request is detected as seen before (forwarded/spiraled/looped) only if self inserted via is found in the message and the value of its branch param plays a key role in detecting loop versus spiral. Hence enabling via insertion becomes a requirement to do loop detection check.
- **max-forwards-check**
  Enables or disables checking on max-forwards. The max-forwards header field serves to limit the number of hops a request can transit on the way to its destination. If 0, the request is discarded. An error response is sent, if configured.
- **max-msg-header-count**
  Indicates the maximum count of expected SIP message header fields. A message that exceeds this limit is silently discarded.
- **max-msg-header-size**
  Indicates the maximum SIP message header size (in bytes). A message which exceeds this size is silently discarded.
- **max-msg-size**
  Indicates the maximum number acceptable SIP message size (in bytes). A message which exceeds this size is silently discarded.

- **name**
  Specifies a unique name for the component. This option is required for the commands **create**, **delete**, and **modify**.
- **partition**
  Displays the administrative partition within which the component resides.
- **persistence**
  Configure the persistence settings.
- **persistence.persist-key**
  Specifies the method which should be used to extract the key value that is used to persist on. The options are:
  - **Call-ID**
    Persist based on the "Call-ID" header field value in the message.
  - **Custom**
    Persist based on the custom key specified using an iRule.
  - **Src-Addr**
    Persist based on originating IP address in the message.

  The default option is **Call-ID**.
- **persistence.persist-timeout**
  Specifies the timeout value of persistence entries in seconds. Upon receiving of the response for the initial SIP Request message, the persistence record is updated with the persist-timeout value.
- **persistence.persist-type**
  Specifies the type of the persistence to be used for the specified "persist-key" attribute value. The options are:
  - **session**
    Persistence is enabled guaranteeing that messages containing a given persistence key will be delivered to the same peer.
  - **none**
    Persistence is disabled.

  The default option is **session**.
- **regex**
  Displays the items that match the regular expression. The regular expression must be preceded by an at sign (@[regular expression]) to indicate that the identifier is a regular expression. See **help regex** for a description of regular expression syntax.
- **enable-sip-firewall**
  Indicates whether to enable the Application Firewall Security policy. When enabled, the configured AFM security features will apply to the virtual server(s) using this SIP session profile.

See Also

create, *delete*, *edit*, glob, *list*, *virtual*, *modify*, regex, *reset-stats*, *show*, *tmsh*

65

ltm monitor

- Introducing the ltm monitor module
- Alphabetical list of components

Introducing the ltm monitor module

You can use the tmsh components that reside within the ltm monitor module to configure Local Traffic Manager™ monitors. For more information about the tmsh hierarchical structure, see Chapter 2, *Understanding and Using the Traffic Management Shell*.

For more information about configuring monitors, refer to the *Configuration Guide for BIG-IP® Local Traffic Manager™*.

Alphabetical list of components

The remainder of this chapter lists the tmsh components that are available in the ltm monitor module.

diameter

Configures a monitor for Diameter protocol resources.

Syntax

Configure the **diameter** component within the **ltm monitor** module using the syntax in the following sections.

Create/Modify

```
create diameter [name]
modify diameter [name]
    acct-application-id [ [integer] | none ]
    app-service [[string] | none]
    auth-application-id [ [integer] | none ]
    defaults-from [name]
    description [string]
    host-ip-address [ [ip address] | none]
    interval [integer]
    manual-resume [enabled | disabled]
    origin-host [ [ip address] | none]
    origin-realm [ [hostname] | none]
    product-name [name]
    time-until-up [integer]
    timeout [integer]
    up-interval [integer]
    vendor-id [integer]
    vendor-specific-acct-application-id [ [integer] | none]
    vendor-specific-auth-application-id [ [integer] | none]
    vendor-specific-vendor-id [ [integer] | none]
edit diameter [ [ [name] | [glob] | [regex] ] ... ]
      all-properties
      non-default-properties
```

Display

```
list diameter
list diameter [ [ [name] | [glob] | [regex] ] ... ]
show diameter [ [ [name] | [glob] | [regex] ] ... ]
show running-config diameter
show running-config diameter [ [ [name] | [glob] | [regex] ] ... ]
    all-properties
    non-default-properties
    one-line
    partition
```

Delete

```
delete diameter [name]
```

◆ Note

You cannot delete default monitors.

Description

You can use the **diameter** component to configure a custom monitor, or you can use the default Diameter monitor that the Local Traffic Manager provides. This type of monitor checks the health of Diameter protocol resources.

Examples

create diameter my_diameter defaults-from diameter

Creates a monitor named **my_diameter** that inherits properties from the default Diameter monitor.

list diameter

Displays the properties of all of the Diameter monitors.

Options

- **acct-application-id**
  Specifies the ID of the accounting portion of a Diameter application. If you specify this option, you must also specify a value for the **auth-application-id** option. The default value is **none**.
  Note that the **acct-application-id** and **auth-application-id** attribute-value-pair (AVP), and the **vendor-specific-auth-application-id** and **vendor-specific-acct-application-id** AVP are mutually exclusive. You can only specify one of these AVPs.
- **app-service**
  Specifies the name of the application service to which the monitor belongs. The default value is **none**. **Note:** If the **strict-updates** option is **enabled** on the application service that owns the object, you cannot modify or delete the monitor. Only the application service can modify or delete the monitor.
- **auth-application-id**
  Specifies the ID of the authentication and authorization portion of a Diameter application. If you specify this option, you must also specify a value for the **acct-application-id** option. The default value is **none**.
  Note that the **acct-application-id** and **auth-application-id** attribute-value-pair (AVP), and the **vendor-specific-auth-application-id** and **vendor-specific-acct-application-id** AVP are mutually exclusive. You can only specify one set of these AVPs.
- **defaults-from**
  Specifies the name of the monitor from which you want your custom monitor to inherit settings. The default value is **firepass**.
- **description**
  User defined description.

- **glob**
  Displays the items that match the **glob** expression. See **help glob** for a description of **glob** expression syntax.
- **host-ip-address**
  Specifies the IP address of the sender of the Diameter message for the Diameter protocol peer discovery feature. The default value is **none**.
- **interval**
  Specifies, in seconds, the frequency at which the system issues the monitor check when either the resource is **down** or the status of the resource is unknown. The default value is **10** seconds.

Important

*F5 Networks recommends that when you configure this option and the **up-interval** option, whichever value is greater be a multiple of the lesser value to allow for an even distribution of monitor checks among all monitors.*

- **manual-resume**
  Specifies whether the system automatically changes the status of a resource to **up** at the next successful monitor check. The default value is **disabled**.
  Note that if you set the **manual-resume** option to **enabled**, you must manually mark the resource as **up** before the system can use it for load balancing connections.
- **name**
  Specifies a unique name for the component. This option is required for the commands **create**, **delete**, and **modify**.
- **origin-host**
  Specifies the IP address from which the Diameter message originates. The default value is **none**.
- **origin-realm**
  Specifies the realm in which the host from which the Diameter message originates resides. The default value is **f5.com**.
- **partition**
  Displays the administrative partition within which the component resides.
- **product-name**
  Specifies the vendor-assigned name of the Diameter application. The value of this option must remain constant across firmware revisions for the same product. The default value is **F5 BIGIP Diameter Health Monitoring**.
- **regex**
  Displays the items that match the regular expression. The regular expression must be preceded by an at sign (@[regular expression]) to indicate that the identifier is a regular expression. See **help regex** for a description of regular expression syntax.

- **time-until-up**
  Specifies the amount of time, in seconds, after the first successful response before a node is marked **up**. A value of **0** (zero) causes a node to be marked **up** immediately after a valid response is received from the node. The default value is **0** (zero).
- **timeout**
  Specifies the number of seconds the target has in which to respond to the monitor request. The default value is **31** seconds.
  If the target responds within the set time period, it is considered **up**. If the target does not respond within the set time period, it is considered **down**. Also, if the target responds with a RESET packet, the system immediately flags the target as **down** without waiting for the timeout interval to expire.
- **up-interval**
  Specifies, in seconds, the frequency at which the system issues the monitor check when the resource is up. The default value is **0** (zero), which specifies that the system uses the value of the interval option whether the resource is **up** or **down**.

Important

*F5 Networks recommends that when you configure this option and the **interval** option, whichever value is greater be a multiple of the lesser value to allow for an even distribution of monitor checks among all monitors.*

- **vendor-id**
  Specifies the IANA SMI Network Management Private Enterprise Code assigned to the vendor of the Diameter application. The default value is **3375**.
- **vendor-specific-acct-application-id**
  Specifies the ID of the vendor-specific accounting portion of a Diameter application. If you specify this option, you must also specify a value for the **vendor-specific-auth-application-id** option. The default value is **none**.
  Note that the **acct-application-id** and **auth-application-id** attribute-value-pair (AVP), and the **vendor-specific-auth-application-id** and **vendor-specific-acct-application-id** AVP are mutually exclusive. You can only specify one of these AVPs.
- **vendor-specific-auth-application-id**
  Specifies the ID of the vendor-specific authentication and authorization portion of a Diameter application. If you specify this option, you must also specify a value for the **vendor-specific-acct-application-id** option. The default value is **none**.
  Note that the **acct-application-id** and **auth-application-id** attribute-value-pair (AVP), and the **vendor-specific-auth-application-id** and **vendor-specific-acct-application-id** AVP are mutually exclusive. You can only specify one of these AVPs.

- **vendor-specific-vendor-id**
  Specifies the ID of a vendor-specific Diameter application. The system uses this ID to advertise support for the application. The default value is **none**.

See Also

create, *delete*, *edit*, glob, *list*, *modify*, regex, *show*, *tmsh*

dns

Configures a Domain Name System (DNS) monitor.

Syntax

Configure the **dns** component within the **ltm monitor** module using the syntax in the following sections.

Create/Modify

```
create dns [name]
modify dns [name]
    accept-rcode [no-error | anything]
    adaptive [enabled | disabled]
    adaptive-divergence-type [relative | absolute]
    adaptive-divergence-value [integer]
    adaptive-limit [integer]
    adaptive-sampling-timespan [integer]
    answer-contains [query-type | any-type | anything]
    app-service [[string] | none]
    defaults-from [name]
    description [string]
    destination [ip address][port]
    interval [integer]
    manual-resume [enabled | disabled]
    qname [string]
    qtype [a | aaaa]
    recv [none | [string] ]
    reverse [enabled | disabled]
    time-until-up [integer]
    timeout [integer]
    transparent [disabled | enabled]
    up-interval [integer]
edit dns [ [ [name] | [glob] | [regex] ] ... ]
    all-properties
    non-default-properties
```

Display

```
list dns
list dns [ [ [name] | [glob] | [regex] ] ... ]
show dns [ [ [name] | [glob] | [regex] ] ... ]
show running-config dns
show running-config dns [ [ [name] | [glob] | [regex] ] ... ]
    all-properties
    non-default-properties
    one-line
    partition
```

Delete

```
delete dns [name]
```

◆ Note

You cannot delete default monitors.

Description

You can use the **dns** component to configure a custom monitor. This type of monitor verifies the DNS service by attempting to send DNS requests generated using the parameters provided to a pool, pool member, or virtual server and validating the DNS response.

Examples

create dns my_dns defaults-from dns qname www.test.com

Creates a monitor named **my_dns** that inherits properties other than qname from the default DNS monitor.

list dns

Displays the properties of all of the DNS monitors.

Options

- **accept_rcode**
  Specifies the RCODE required in the response for an 'up' status. The default value is **no-error**.
  The options are:
  - **no-error**
    Specifies that the status of the node will be marked up if the received dns message has RCODE = NOERROR.
  - **anything**
    Specifies that the status of the node will be marked up irrespective of the RCODE in the dns message received.
- **adaptive**
  Specifies whether the adaptive feature is enabled for this monitor. Not all monitors support the adaptive feature.
- **adaptive-divergence-type**
  Specifies whether the *adaptive-divergence-value* is **relative** or **absolute**.
- **adaptive-divergence-value**
  Specifies how far from mean latency each monitor probe is allowed to be. If *adaptive-divergence-type* is *relative*, this value is a percentage deviation from mean (e.g. 50 would indicate the probe is allowed to exceed the mean latency by 50%.) If *adaptive-divergence-type* is *absolute*, this value is an offset from mean in milliseconds (e.g. 250

would indicate the probe is allowed allowed to exceed the mean latency by 250 ms.) A probe that exceeds latency is counted the same as a probe that is not received, so in the typical scenario, it will require three missed latencies in a row to mark a pool member or node down (i.e. a 15-second interval with a 46-second timeout, would require three missed probes before the pool member or node would be marked down.)

- **adaptive-limit**
  Specifies the hard limit, in milliseconds, which the probe is not allowed to exceed, regardless of the divergence value. For example, if this value is 500, then the probe latency may not exceed 500 ms even if that would still fall within the divergence value.
- **adaptive-sampling-timespan**
  Specifies the size of the sliding window, in seconds, which records probe history. For example, if this value is 300, then a sliding window of the last five minutes' probe history will be used for calculating probe mean latency and standard deviation.
- **answer_contains**
  Specifies the record types required in the answer section of the response in order to mark the status of a node up. The default value is **query-type**. The options are:
  - **query-type**
    Specifies that the response should contain at least one answer of which the resource record type matches the qtype.
  - **any-type**
    Specifies that the dns message should contain at least one answer.
  - **anything**
    Specifies that an empty answer section is enough to mark the status of the node up.
- **app-service**
  Specifies the name of the application service to which the monitor belongs. The default value is **none**. **Note:** If the **strict-updates** option is **enabled** on the application service that owns the object, you cannot modify or delete the monitor. Only the application service can modify or delete the monitor.
- **defaults-from**
  Specifies the name of the monitor from which you want your custom monitor to inherit settings. The default value is **dns**.
- **description**
  User defined description.
- **destination**
  Specifies the IP address and service port of the resource that is the destination of this monitor. Possible values are:
  - ***:***
    Specifies to perform a health check on the IP address and port supplied by a pool member.

- ***:port**
  Specifies to perform a health check on the server with the IP address supplied by the pool member and the port you specify.
- **IP address:port**
  Specifies to mark a pool member **up** or **down** based on the response of the server at the IP address and port you specify.
- **IP address:port** (with the **transparent** option **enabled**)
  Specifies to perform a health check on the server at the IP address and port you specify, route the check through the IP address and port supplied by the pool member, and mark the pool member (the gateway) **up** or **down** accordingly.

◆ **glob**
Displays the items that match the **glob** expression. See **help glob** for a description of **glob** expression syntax.

◆ **interval**
Specifies, in seconds, the frequency at which the system issues the monitor check when either the resource is **down** or the status of the resource is unknown. The default value is **5** seconds.

Important

*F5 Networks recommends that when you configure this option and the **up-interval** option, whichever value is greater be a multiple of the lesser value to allow for an even distribution of monitor checks among all monitors.*

◆ **manual-resume**
Specifies whether the system automatically changes the status of a resource to **up** at the next successful monitor check. The default value of the manual-resume option is **disabled**.
Note that if you set the **manual-resume** option to **enabled**, you must manually mark the resource as **up** before the system can use it for load balancing connections.

◆ **name**
Specifies a unique name for the component. This option is required for the commands **create**, **delete**, and **modify**.

◆ **partition**
Displays the administrative partition within which the component resides.

◆ **qname**
Specifies the query name that the monitor send a DNS query for. The default value is **Enter a query name**.

◆ **qtype**
Specifies the query type of that the monitor sends a query. The default value is **a**.
The options are:

- **a**
  Specifies that the monitor will send a DNS query of type A.

- **aaaa**
  Specifies that the monitor will send a DNS query of type AAAA.

- **recv**
  Specifies the ip address that the monitor looks for in the dns response's resource record sections. The ip address should be specified in the dotted-decimal notation or ipv6 notation. The default value is **none**. If no recv value is specified, then the dns message will be checked against accept_rcode and answer_contains monitor parameters respectively.
- **regex**
  Displays the items that match the regular expression. The regular expression must be preceded by an at sign (@[regular expression]) to indicate that the identifier is a regular expression. See **help regex** for a description of regular expression syntax.
- **reverse**
  Specifies whether the monitor operates in reverse mode. When the monitor is in reverse mode, a successful receive string match marks the monitored object **down** instead of **up**. You can use the this mode only if you configure **recv** option.
  The default value is **disabled**, which specifies that the monitor does not operate in reverse mode. The **enabled** value specifies that the monitor operates in reverse mode.
- **time-until-up**
  Specifies the amount of time, in seconds, after the first successful response before a node is marked **up**. A value of **0** (zero) causes a node to be marked **up** immediately after a valid response is received from the node. The default value is **0** (zero).
- **timeout**
  Specifies the number of seconds the target has in which to respond to the monitor request. The default value is **16** seconds. If the target responds within the set time period, it is considered up. If the target does not respond within the set time period, it is considered down. Also, if the target responds with a RESET packet, the system immediately flags the target as down without waiting for the timeout interval to expire.
- **transparent**
  Specifies whether the monitor operates in transparent mode. Monitors in transparent mode can monitor pool members through firewalls. The default value is **disabled**.
- **up-interval**
  Specifies, in seconds, the frequency at which the system issues the monitor check when the resource is **up**. The default value is **0** (zero), which specifies that the system uses the value of the **interval** option whether the resource is **up** or **down**.

Important

*F5 Networks recommends that when you configure this option and the **interval** option, whichever value is greater be a multiple of the lesser value to allow for an even distribution of monitor checks among all monitors.*

See Also

create, *delete*, *edit*, glob, *list*, *modify*, regex, *show*, *tmsh*

external

Configures an external monitor.

Syntax

Configure the **external** component within the **ltm monitor** module using the syntax in the following sections.

Create/Modify

```
create external [name]
modify external [name]
    args [ [arguments] | none]
    app-service [[string] | none]
    defaults-from [name]
    description [string]
    destination [ip address][port]
    interval [integer]
    manual-resume [enabled | disabled]
    run [none | [path] ]
    time-until-up [integer]
    timeout [integer]
    user-defined [ [name] [value] | [name] none ]
    up-interval [integer]
edit external [ [ [name] | [glob] | [regex] ] ... ]
    all-properties
    non-default-properties
```

Display

```
list external
list external [ [ [name] | [glob] | [regex] ] ... ]
show external [ [ [name] | [glob] | [regex] ] ... ]
show running-config external
show running-config external [ [ [name] | [glob] | [regex] ] ... ]
    all-properties
    non-default-properties
    one-line
    partition
```

Delete

```
delete external [name]
```

◆ Note

You cannot delete default monitors.

Description

You can use the **external** component to configure a custom monitor, or you can use the default external monitor that the Local Traffic Manager provides. Using this type of monitor, you can use your own programs to monitor services.

Examples

create external my_external defaults-from external

Creates a monitor named my_external that inherits properties from the default external monitor.

list external

Displays the properties of all of the external monitors.

Options

- **args**
  Specifies any command-line arguments that the external program requires. The default value is **none**.
- **app-service**
  Specifies the name of the application service to which the monitor belongs. The default value is **none**. **Note:** If the **strict-updates** option is **enabled** on the application service that owns the object, you cannot modify or delete the monitor. Only the application service can modify or delete the monitor.
- **defaults-from**
  Specifies the name of the monitor from which you want your custom monitor to inherit settings. The default value is **external**.
- **description**
  User defined description.
- **destination**
  Specifies the IP address and service port of the resource that is the destination of this monitor. The default value is ***:***.
  Possible values are:
  - ***:***
    Specifies to perform a health check on the address and port supplied by a pool member.
  - ***:port**
    Specifies to perform a health check on the server with the IP address supplied by the pool member and the port you specify.
  - **IP address:port**
    Specifies to mark a pool member **up** or **down** based on the response of the server at the IP address and port you specify.

- **glob**
  Displays the items that match the **glob** expression. See **help glob** for a description of **glob** expression syntax.
- **interval**
  Specifies, in seconds, the frequency at which the system issues the monitor check when either the resource is **down** or the status of the resource is unknown. The default value is **5** seconds.

Important

*F5 Networks recommends that when you configure this option and the **up-interval** option, whichever value is greater be a multiple of the lesser value to allow for an even distribution of monitor checks among all monitors.*

- **manual-resume**
  Specifies whether the system automatically changes the status of a resource to **up** at the next successful monitor check. The default value of the manual-resume option is **disabled**.
  Note that if you set the **manual-resume** option to **enabled**, you must manually mark the resource as **up** before the system can use it for load balancing connections.
- **name**
  Specifies a unique name for the component. This option is required for the commands **create**, **delete**, and **modify**.
- **partition**
  Displays the administrative partition within which the component resides.
- **regex**
  Displays the items that match the regular expression. The regular expression must be preceded by an at sign (@[regular expression]) to indicate that the identifier is a regular expression. See **help regex** for a description of regular expression syntax.
- **run**
  Specifies the path and file name of a program to run as the external monitor, for example **/config/monitors/myMonitor**. The default value is **none**.
- **time-until-up**
  Specifies the amount of time, in seconds, after the first successful response before a node is marked **up**. A value of **0** (zero) causes a node to be marked **up** immediately after a valid response is received from the node. The default value is **0** (zero).
- **timeout**
  Specifies the number of seconds the target has in which to respond to the monitor request. The default value is **16** seconds.
  If the target responds within the set time period, it is considered **up**. If the target does not respond within the set time period, it is considered **down**.

Also, if the target responds with a RESET packet, the system immediately flags the target as **down** without waiting for the timeout interval to expire.

- **up-interval**
  Specifies, in seconds, the frequency at which the system issues the monitor check when the resource is **up**. The default value is **0** zero, which specifies that the system uses the value of the **interval** option whether the resource is **up** or **down**.

Important

*F5 Networks recommends that when you configure this option and the **interval** option, whichever value is greater be a multiple of the lesser value to allow for an even distribution of monitor checks among all monitors.*

- **user-defined**
  Specifies any user-defined command-line arguments and variables that the external program requires. Use the following syntax to specify a user defined parameter.

modify external my_external user-defined my_param_name my_param_value

Use the following syntax to remove a user defined parameter.

modify external my_external user-defined my_param_name none

See Also

create, *delete*, *edit*, glob, *list*, *modify*, regex, *show*, *tmsh*

firepass

Configures a FirePass® monitor.

Syntax

Configure the **firepass** component within the **ltm monitor** module using the syntax in the following sections.

Create/Modify

```
create firepass [name]
modify firepass [name]
    app-service [[string] | none]
    cipherlist [list]
    concurrency-limit [integer]
    defaults-from [name]
    description [string]
    destination [ip address][port]
    interval [integer]
    max-load-average [integer]
    password [password]
    time-until-up [integer]
    timeout [integer]
    up-interval [integer]
    username [ [name] | none]
edit firepass [ [ [name] | [glob] | [regex] ] ... ]
      all-properties
      non-default-properties
```

Display

```
list firepass
list firepass [ [ [name] | [glob] | [regex] ] ... ]
show firepass [ [ [name] | [glob] | [regex] ] ... ]
show running-config firepass
show running-config firepass [ [ [name] | [glob] | [regex] ] ... ]
    all-properties
    non-default-properties
    one-line
    partition
```

Delete

```
delete firepass [name]
```

◆ Note

You cannot delete default monitors.

Description

You can use the **firepass** component to configure a custom monitor, or you can use the default Firepass monitor that the Local Traffic Manager provides. This type of monitor checks the health of FirePass systems.

Examples

create firepass my_firepass defaults-from firepass

Creates a monitor named **my_firepass** that inherits properties from the default Firepass monitor.

list firepass

Displays the properties of all of the Firepass monitors.

Options

- **app-service**
  Specifies the name of the application service to which the monitor belongs. The default value is **none**. **Note:** If the **strict-updates** option is **enabled** on the application service that owns the object, you cannot modify or delete the monitor. Only the application service can modify or delete the monitor.
- **cipherlist**
  Specifies the list of ciphers for this monitor. The default value is **HIGH:!ADH**.
- **concurrency-limit**
  Specifies the maximum percentage of licensed connections currently in use under which the monitor marks the FirePass system **up**. The default value is **95**.
  For example, a value of 95 percent means that the monitor marks the FirePass system **up** until 95 percent of licensed connections are in use. When the number of in-use licensed connections exceeds 95 percent, the monitor marks the FirePass system **down**.
- **defaults-from**
  Specifies the name of the monitor from which you want your custom monitor to inherit settings. The default value is **firepass**.
- **description**
  User defined description.
- **destination**
  Specifies the IP address and service port of the resource that is the destination of this monitor. The default value is ***:***.
  Possible values are:
  - ***:***
    Specifies to perform a health check on the address and port supplied by a pool member.

- ***:port**
  Specifies to perform a health check on the server with the IP address supplied by the pool member and the port you specify.
- **IP address:port**
  Specifies to mark a pool member **up** or **down** based on the response of the server at the IP address and port you specify.

- **glob**
  Displays the items that match the **glob** expression. See **help glob** for a description of **glob** expression syntax.
- **interval**
  Specifies, in seconds, the frequency at which the system issues the monitor check when either the resource is **down** or the status of the resource is unknown. The default value is **5** seconds.

Important

*F5 Networks recommends that when you configure this option and the **up-interval** option, whichever value is greater be a multiple of the lesser value to allow for an even distribution of monitor checks among all monitors.*

- **name**
  Specifies a unique name for the component. This option is required for the commands **create**, **delete**, and **modify**.
- **max-load-average**
  Specifies the number that the monitor uses to mark the FirePass system **up** or **down**. The system compares the value of this option to a one-minute average of the FirePass system load. When the FirePass system-load average falls within the specified value, the monitor marks the FirePass system **up**. When the average exceeds the value, the monitor marks the system **down**.
  The default value is **12.0**.
- **name**
  Specifies a unique name for the component. This option is required for the commands **create**, **delete**, and **modify**.
- **partition**
  Displays the administrative partition within which the component resides.
- **password**
  Specifies the password, if the monitored target requires authentication. The default value is **none**.
- **regex**
  Displays the items that match the regular expression. The regular expression must be preceded by an at sign (@[regular expression]) to indicate that the identifier is a regular expression. See **help regex** for a description of regular expression syntax.

- **time-until-up**
  Specifies the amount of time, in seconds, after the first successful response before a node is marked **up**. A value of **0** (zero) causes a node to be marked **up** immediately after a valid response is received from the node. The default value is **0** (zero).
- **timeout**
  Specifies the number of seconds the target has in which to respond to the monitor request. The default value is **16** seconds.
  If the target responds within the set time period, it is considered **up**. If the target does not respond within the set time period, it is considered **down**. Also, if the target responds with a RESET packet, the system immediately flags the target as **down** without waiting for the timeout interval to expire.
- **up-interval**
  Specifies, in seconds, the frequency at which the system issues the monitor check when the resource is **up**. The default value is **0** (zero), which specifies that the system uses the value of the **interval** option whether the resource is **up** or **down**.

Important

*F5 Networks recommends that when you configure this option and the **interval** option, whichever value is greater be a multiple of the lesser value to allow for an even distribution of monitor checks among all monitors.*

- **username**
  Specifies the username, if the monitored target requires authentication. The default value is **gtmuser**.

See Also

create, *delete*, *edit*, glob, *list*, *modify*, regex, *show*, *tmsh*

ftp

Configures a File Transfer Protocol (FTP) monitor.

Syntax

Configure the **ftp** component within the **ltm monitor** module using the syntax in the following sections.

Create/Modify

```
create ftp [name]
modify ftp [name]
    adaptive [enabled | disabled]
    adaptive-divergence-type [relative | absolute]
    adaptive-divergence-value [integer]
    adaptive-limit [integer]
    adaptive-sampling-timespan [integer]
    app-service [[string] | none]
    debug [no | yes]
    defaults-from [name]
    description [string]
    destination [ip address][port]
    filename [ [filename] | none]
    interval [integer]
    manual-resume [enabled | disabled]
    mode [passive | port]
    password [none | [password] ]
    time-until-up [integer]
    timeout [integer]
    up-interval [integer]
    username [name]
edit ftp [ [ [name] | [glob] | [regex] ] ... ]
    all-properties
    non-default-properties
```

Display

```
list ftp
list ftp [ [ [name] | [glob] | [regex] ] ... ]
show ftp [ [ [name] | [glob] | [regex] ] ... ]
show running-config ftp
show running-config ftp [ [ [name] | [glob] | [regex] ] ... ]
    all-properties
    non-default-properties
    one-line
    partition
```

Delete

```
delete ftp [name]
```

◆ Note

You cannot delete default monitors.

Description

You can use the **ftp** component to configure a custom monitor, or you can use the default FTP monitor that the Local Traffic Manager provides. This type of monitor verifies the FTP service by attempting to download a specific file to the **/var/tmp** directory on the system. Once downloaded successfully, the file is not saved.

Examples

create ftp my_ftp defaults-from ftp

Creates a monitor named **my_ftp** that inherits properties from the default FTP monitor.

list ftp

Displays the properties of all of the FTP monitors.

Options

- **adaptive**
  Specifies whether the adaptive feature is enabled for this monitor. Not all monitors support the adaptive feature.
- **adaptive-divergence-type**
  Specifies whether the *adaptive-divergence-value* is **relative** or **absolute**.
- **adaptive-divergence-value**
  Specifies how far from mean latency each monitor probe is allowed to be. If *adaptive-divergence-type* is *relative*, this value is a percentage deviation from mean (e.g. 50 would indicate the probe is allowed to exceed the mean latency by 50%.) If *adaptive-divergence-type* is *absolute*, this value is an offset from mean in milliseconds (e.g. 250 would indicate the probe is allowed allowed to exceed the mean latency by 250 ms.) A probe that exceeds latency is counted the same as a probe that is not received, so in the typical scenario, it will require three missed latencies in a row to mark a pool member or node down (i.e. a 15-second interval with a 46-second timeout, would require three missed probes before the pool member or node would be marked down.)
- **adaptive-limit**
  Specifies the hard limit, in milliseconds, which the probe is not allowed to exceed, regardless of the divergence value. For example, if this value is 500, then the probe latency may not exceed 500 ms even if that would still fall within the divergence value.
- **adaptive-sampling-timespan**
  Specifies the size of the sliding window, in seconds, which records probe history. For example, if this value is 300, then a sliding window of the last five minutes' probe history will be used for calculating probe mean latency and standard deviation.

- **app-service**
  Specifies the name of the application service to which the monitor belongs. The default value is **none**. **Note:** If the **strict-updates** option is **enabled** on the application service that owns the object, you cannot modify or delete the monitor. Only the application service can modify or delete the monitor.
- **debug**
  Specifies whether the monitor sends error messages and additional information to a log file created and labeled specifically for this monitor. You can use the log information to help diagnose and troubleshoot unsuccessful health checks.
  The default value is **no**. The options are:
  - **no**
    Specifies that the system does not redirect error messages and additional information related to this monitor.
  - **yes**
    Specifies that the system redirects error messages and additional information to the /var/log/monitors/<monitor_name>-<node_name>-<port>.log file.
- **defaults-from**
  Specifies the name of the monitor from which you want your custom monitor to inherit settings. The default value is **ftp**.
- **description**
  User defined description.
- **destination**
  Specifies the IP address and service port of the resource that is the destination of this monitor. The default value is ***:***.
  Possible values are:
  - ***:***
    Specifies to perform a health check on the address and port supplied by a pool member.
  - ***:port**
    Specifies to perform a health check on the server with the IP address supplied by the pool member and the port you specify.
  - **IP address:port**
    Specifies to mark a pool member **up** or **down** based on the response of the server at the IP address and port you specify.
- **filename**
  Specifies the full path and file name of the file that the system attempts to download. The health check is successful if the system can download the file. The default value is **none**.
- **glob**
  Displays the items that match the **glob** expression. See **help glob** for a description of **glob** expression syntax.

- **interval**
  Specifies, in seconds, the frequency at which the system issues the monitor check when either the resource is **down** or the status of the resource is unknown. The default value is **5** seconds.

Important

*F5 Networks recommends that when you configure this option and the **up-interval** option, whichever value is greater be a multiple of the lesser value to allow for an even distribution of monitor checks among all monitors.*

- **manual-resume**
  Specifies whether the system automatically changes the status of a resource to **up** at the next successful monitor check. The default value of the manual-resume option is **disabled**.
  Note that if you set the **manual-resume** option to **enabled**, you must manually mark the resource as **up** before the system can use it for load balancing connections.
- **mode**
  Specifies the data transfer process (DTP) mode. The default value is **passive**.
  The options are:
  - **passive**
    Specifies that the monitor sends a data transfer request to the FTP server. When the FTP server receives the request, the FTP server then starts and establishes the data connection.
  - **port**
    Specifies that the monitor starts and establishes the data connection with the FTP server.
- **name**
  Specifies a unique name for the component. This option is required for the commands **create**, **delete**, and **modify**.
- **password**
  Specifies the password, if the monitored target requires authentication. The default value is **none**.
- **partition**
  Displays the administrative partition within which the component resides.
- **regex**
  Displays the items that match the regular expression. The regular expression must be preceded by an at sign (@[regular expression]) to indicate that the identifier is a regular expression. See **help regex** for a description of regular expression syntax.
- **time-until-up**
  Specifies the amount of time, in seconds, after the first successful response before a node is marked **up**. A value of **0** (zero) causes a node to be marked **up** immediately after a valid response is received from the node. The default value is **0** (zero).

- **timeout**
  Specifies the number of seconds the target has in which to respond to the monitor request. The default value is **31** seconds.
  If the target responds within the set time period, it is considered **up**. If the target does not respond within the set time period, it is considered **down**. Also, if the target responds with a RESET packet, the system immediately flags the target as **down** without waiting for the timeout interval to expire.
- **up-interval**
  Specifies, in seconds, the frequency at which the system issues the monitor check when the resource is **up**. The default value is **0** zero, which specifies that the system uses the value of the **interval** option whether the resource is **up** or **down**.

Important

*F5 Networks recommends that when you configure this option and the **interval** option, whichever value is greater be a multiple of the lesser value to allow for an even distribution of monitor checks among all monitors.*

- **username**
  Specifies the username, if the monitored target requires authentication. The default value is **none**.

See Also

create, *delete*, *edit*, glob, *list*, *modify*, regex, *show*, *tmsh*

gateway-icmp

Configures a Gateway Internet Control Message Protocol (ICMP) monitor.

Syntax

Configure the **gateway-icmp** component within the **ltm monitor** module using the syntax in the following sections.

Create/Modify

```
create gateway-icmp [name]
modify gateway-icmp [name]
    adaptive [enabled | disabled]
    adaptive-divergence-type [relative | absolute]
    adaptive-divergence-value [integer]
    adaptive-limit [integer]
    adaptive-sampling-timespan [integer]
    app-service [[string] | none]
    defaults-from [name]
    description [string]
    destination [ip address][port]
    interval [integer]
    manual-resume [enabled | disabled]
    time-until-up [integer]
    timeout [integer]
    transparent [enabled | disabled]
    up-interval [integer]
edit gateway-icmp [ [ [name] | [glob] | [regex] ] ... ]
    all-properties
    non-default-properties
```

Display

```
list gateway-icmp
list gateway-icmp [ [ [name] | [glob] | [regex] ] ... ]
show gateway-icmp [ [ [name] | [glob] | [regex] ] ... ]
show running-config gateway-icmp
show running-config gateway-icmp [ [ [name] | [glob] | [regex] ] ... ]
    all-properties
    non-default-properties
    one-line
    partition
```

Delete

```
delete gateway-icmp [name]
```

◆ Note

You cannot delete default monitors.

Description

You can use the **gateway-icmp** component to configure a custom monitor, or you can use the default Gateway ICMP monitor that the Local Traffic Manager provides. This type of monitor monitors a pool that implements gateway fail-safe for high availability.

Examples

create gateway-icmp my_imcp defaults-from gateway_icmp

Creates a monitor named **my_icmp** that inherits properties from the default Gateway ICMP monitor.

list gateway-icmp

Displays the properties of all of the Gateway ICMP monitors.

Options

- **adaptive**
  Specifies whether the adaptive feature is enabled for this monitor. Not all monitors support the adaptive feature.
- **adaptive-divergence-type**
  Specifies whether the *adaptive-divergence-value* is **relative** or **absolute**.
- **adaptive-divergence-value**
  Specifies how far from mean latency each monitor probe is allowed to be. If *adaptive-divergence-type* is *relative*, this value is a percentage deviation from mean (e.g. 50 would indicate the probe is allowed to exceed the mean latency by 50%.) If *adaptive-divergence-type* is *absolute*, this value is an offset from mean in milliseconds (e.g. 250 would indicate the probe is allowed allowed to exceed the mean latency by 250 ms.) A probe that exceeds latency is counted the same as a probe that is not received, so in the typical scenario, it will require three missed latencies in a row to mark a pool member or node down (i.e. a 15-second interval with a 46-second timeout, would require three missed probes before the pool member or node would be marked down.)
- **adaptive-limit**
  Specifies the hard limit, in milliseconds, which the probe is not allowed to exceed, regardless of the divergence value. For example, if this value is 500, then the probe latency may not exceed 500 ms even if that would still fall within the divergence value.
- **adaptive-sampling-timespan**
  Specifies the size of the sliding window, in seconds, which records probe history. For example, if this value is 300, then a sliding window of the last five minutes' probe history will be used for calculating probe mean latency and standard deviation.

- **app-service**
  Specifies the name of the application service to which the monitor belongs. The default value is **none**. **Note:** If the **strict-updates** option is **enabled** on the application service that owns the object, you cannot modify or delete the monitor. Only the application service can modify or delete the monitor.
- **defaults-from**
  Specifies the name of the monitor from which you want your custom monitor to inherit settings. The default value is **gateway_icmp**.
- **description**
  User defined description.
- **destination**
  Specifies the IP address and service port of the resource that is the destination of this monitor. The default value is ***:***.
  Possible values are:
  - ***:***
    Specifies to perform a health check on the IP address and port supplied by a pool member.
  - ***:port**
    Specifies to perform a health check on the server with the IP address supplied by the pool member and the port you specify.
  - **IP address:port**
    Specifies to mark a pool member **up** or **down** based on the response of the server at the IP address and port you specify.
  - **IP address:port** (with the **transparent** option **enabled**)
    Specifies to perform a health check on the server at the IP address and port specified in the monitor, routing the check through the IP address and port supplied by the pool member. The pool member (the gateway) is marked **up** or **down** accordingly.
- **glob**
  Displays the items that match the **glob** expression. See **help glob** for a description of **glob** expression syntax.
- **interval**
  Specifies, in seconds, the frequency at which the system issues the monitor check when either the resource is **down** or the status of the resource is unknown. The default value is **5** seconds.

Important

*F5 Networks recommends that when you configure this option and the **up-interval** option, whichever value is greater be a multiple of the lesser value to allow for an even distribution of monitor checks among all monitors.*

- **manual-resume**
  Specifies whether the system automatically changes the status of a resource to **up** at the next successful monitor check. The default value of the manual-resume option is **disabled**.

Note that if you set the **manual-resume** option to **enabled**, you must manually mark the resource as **up** before the system can use it for load balancing connections.

- **name**
  Specifies a unique name for the component. This option is required for the commands **create**, **delete**, and **modify**.
- **partition**
  Displays the administrative partition within which the component resides.
- **regex**
  Displays the items that match the regular expression. The regular expression must be preceded by an at sign (@[regular expression]) to indicate that the identifier is a regular expression. See **help regex** for a description of regular expression syntax.
- **time-until-up**
  Specifies the amount of time, in seconds, after the first successful response before a node is marked **up**. A value of **0** (zero) causes a node to be marked **up** immediately after a valid response is received from the node. The default value is **0** (zero).
- **timeout**
  Specifies the number of seconds the target has in which to respond to the monitor request. The default value is **16** seconds.
  If the target responds within the set time period, it is considered **up**. If the target does not respond within the set time period, it is considered **down**. Also, if the target responds with a RESET packet, the system immediately flags the target as **down** without waiting for the timeout interval to expire.
- **transparent**
  Specifies whether the monitor operates in transparent mode. Monitors in transparent mode can monitor pool members through firewalls. The default value is **disabled**.
- **up-interval**
  Specifies, in seconds, the frequency at which the system issues the monitor check when the resource is **up**. The default value is **0** (zero), which specifies that the system uses the value of the **interval** option whether the resource is **up** or **down**.

Important

*F5 Networks recommends that when you configure this option and the **interval** option, whichever value is greater be a multiple of the lesser value to allow for an even distribution of monitor checks among all monitors.*

See Also

create, *delete*, *edit*, glob, *list*, *modify*, regex, *show*, *tmsh*

http

Configures a Hypertext Transfer Protocol (HTTP) monitor.

Syntax

Configure the **http** component within the **ltm monitor** module using the syntax in the following sections.

Create/Modify

```
create http [name]
modify http [name]
    adaptive [enabled | disabled]
    adaptive-divergence-type [relative | absolute]
    adaptive-divergence-value [integer]
    adaptive-limit [integer]
    adaptive-sampling-timespan [integer]
    app-service [[string] | none]
    defaults-from [name]
    description [string]
    destination [ip address][port]
    interval [integer]
    ip-tos [integer]
    manual-resume [enabled | disabled]
    password [none | [password] ]
    recv [none | [string] ]
    recv-disable [none | [string] ]
    reverse [enabled | disabled]
    ip-dscp [integer]
    send [none | [string] ]
    time-until-up [integer]
    timeout [integer]
    transparent [enabled | disabled]
    up-interval [integer]
    username [ [name] | none]
edit http [ [ [name] | [glob] | [regex] ] ... ]
    all-properties
    non-default-properties
```

Display

```
list http
list http [ [ [name] | [glob] | [regex] ] ... ]
show http [ [ [name] | [glob] | [regex] ] ... ]
show running-config http
show running-config http [ [ [name] | [glob] | [regex] ] ... ]
    all-properties
    non-default-properties
    one-line
    partition
```

Delete

```
delete http [name]
```

◆ Note

You cannot delete default monitors.

Description

You can use the **http** component to configure a custom monitor, or you can use the default HTTP monitor that the Local Traffic Manager provides. This type of monitor verifies the HTTP service by attempting to receive specific content from a Web page.

Examples

create http my_http defaults-from http

Creates a monitor named **my_http** that inherits properties from the default HTTP monitor.

list http

Displays the properties of all of the HTTP monitors.

Options

- **adaptive**
  Specifies whether the adaptive feature is enabled for this monitor. Not all monitors support the adaptive feature.
- **adaptive-divergence-type**
  Specifies whether the *adaptive-divergence-value* is **relative** or **absolute**.
- **adaptive-divergence-value**
  Specifies how far from mean latency each monitor probe is allowed to be. If *adaptive-divergence-type* is *relative*, this value is a percentage deviation from mean (e.g. 50 would indicate the probe is allowed to exceed the mean latency by 50%.) If *adaptive-divergence-type* is *absolute*, this value is an offset from mean in milliseconds (e.g. 250 would indicate the probe is allowed allowed to exceed the mean latency by 250 ms.) A probe that exceeds latency is counted the same as a probe that is not received, so in the typical scenario, it will require three missed latencies in a row to mark a pool member or node down (i.e. a 15-second interval with a 46-second timeout, would require three missed probes before the pool member or node would be marked down.)

- **adaptive-limit**
  Specifies the hard limit, in milliseconds, which the probe is not allowed to exceed, regardless of the divergence value. For example, if this value is 500, then the probe latency may not exceed 500 ms even if that would still fall within the divergence value.
- **adaptive-sampling-timespan**
  Specifies the size of the sliding window, in seconds, which records probe history. For example, if this value is 300, then a sliding window of the last five minutes' probe history will be used for calculating probe mean latency and standard deviation.
- **app-service**
  Specifies the name of the application service to which the monitor belongs. The default value is **none**. **Note:** If the **strict-updates** option is **enabled** on the application service that owns the object, you cannot modify or delete the monitor. Only the application service can modify or delete the monitor.
- **defaults-from**
  Specifies the name of the monitor from which you want your custom monitor to inherit settings. The default value is **http**.
- **description**
  User defined description.
- **destination**
  Specifies the IP address and service port of the resource that is the destination of this monitor. The default value is ***:***.
  Possible values are:
  - ***:***
    Specifies to perform a health check on the IP address and port supplied by a pool member.
  - ***:port**
    Specifies to perform a health check on the server with the IP address supplied by the pool member and the port you specify.
  - **IP address:port**
    Specifies to mark a pool member **up** or **down** based on the response of the server at the IP address and port you specify.
  - **IP address:port** (with the **transparent** option **enabled**)
    Specifies to perform a health check on the server at the IP address and port specified in the monitor, routing the check through the IP address and port supplied by the pool member. The pool member (the gateway) is marked up or down accordingly.
- **glob**
  Displays the items that match the **glob** expression. See **help glob** for a description of **glob** expression syntax.

- **interval**
  Specifies, in seconds, the frequency at which the system issues the monitor check when either the resource is **down** or the status of the resource is unknown. The default value is **5** seconds.

Important

*F5 Networks recommends that when you configure this option and the **up-interval** option, whichever value is greater be a multiple of the lesser value to allow for an even distribution of monitor checks among all monitors.*

- **ip-dscp**
  Specifies the differentiated services code point (DSCP). DSCP is a 6-bit value in the Differentiated Services (DS) field of the IP header. It can be used to specify the quality of service desired for the packet. The valid range for this value is 0 to 63 (hex 0x0 to 0x3f). The default value is zero.
- **manual-resume**
  Specifies whether the system automatically changes the status of a resource to **up** at the next successful monitor check. The default value of the manual-resume option is **disabled**.
  Note that if you set the **manual-resume** option to **enabled**, you must manually mark the resource as **up** before the system can use it for load balancing connections.
- **name**
  Specifies a unique name for the component. This option is required for the commands **create**, **delete**, and **modify**.
- **partition**
  Displays the administrative partition within which the component resides.
- **password**
  Specifies the password if the monitored target requires authentication. The default value is **none**.
- **recv**
  Specifies the text string that the monitor looks for in the returned resource. The default value is **none**.
  The most common receive expressions contain a text string that is included in an HTML file on your site. The text string can be regular text, HTML tags, or image names, and the associated operation is not case-sensitive. If you do not specify a value for both the **send** and **recv** options, the monitor performs a simple service check and connect only.
- **recv-disable**
  Specifies a text string that the monitor looks for in the returned resource. If the text string is matched in the returned resource, the corresponding node or pool member is marked session disabled. The default value is **none**.
  You specify a **recv-disable** string in the same way that you specify a **recv** string.

If you specify a **recv-disable** string, you must also specify a **recv** string. You cannot specify a **recv-disable** string, if the **reverse** option is **enabled**.

- **regex**
  Displays the items that match the regular expression. The regular expression must be preceded by an at sign (@[regular expression]) to indicate that the identifier is a regular expression. See **help regex** for a description of regular expression syntax.
- **reverse**
  Specifies whether the monitor operates in reverse mode. When the monitor is in reverse mode, a successful check marks the monitored object **down** instead of **up**. You can use the this mode only if you configure both the **send** and **recv** options.
  The default value is **disabled**, which specifies that the monitor does not operate in reverse mode. The **enabled** value specifies that the monitor operates in reverse mode.
- **send**
  Specifies the text string that the monitor sends to the target object.
  The default setting is **GET /**, which retrieves a default HTML file for a web site. To retrieve a specific page from a web site, specify a fully-qualified path name, for example, **GET /www/company/index.html**.
  Since the string may have special characters, the system may require that the string be enclosed with single quotation marks.
  If this value is null, then a valid connection suffices to determine that the service is **up**. In this case, the system does not need the **recv** option and ignores the option even if not null.
- **time-until-up**
  Specifies the amount of time, in seconds, after the first successful response before a node is marked **up**. A value of **0** (zero) causes a node to be marked **up** immediately after a valid response is received from the node. The default value is **0** (zero).
- **timeout**
  Specifies the number of seconds the target has in which to respond to the monitor request. The default value is **16** seconds.
  If the target responds within the set time period, it is considered **up**. If the target does not respond within the set time period, it is considered **down**. Also, if the target responds with a RESET packet, the system immediately flags the target as **down** without waiting for the timeout interval to expire.
- **transparent**
  Specifies whether the monitor operates in transparent mode. Monitors in transparent mode can monitor pool members through firewalls. The default value is **disabled**.

- **up-interval**
  Specifies, in seconds, the frequency at which the system issues the monitor check when the resource is **up**. The default value is **0** (zero), which specifies that the system uses the value of the **interval** option whether the resource is **up** or **down**.

Important

*F5 Networks recommends that when you configure this option and the **interval** option, whichever value is greater be a multiple of the lesser value to allow for an even distribution of monitor checks among all monitors.*

- **username**
  Specifies the username, if the monitored target requires authentication. The default value is **none**.

See Also

create, *delete*, *edit*, glob, *list*, *modify*, regex, *show*, *tmsh*

https

Configures a Hypertext Transfer Protocol over Secure Socket Layer (HTTPS) monitor.

Syntax

Configure the **https** component within the **ltm monitor** module using the syntax in the following sections.

Create/Modify

```
create https [name]
modify https [name]
    adaptive [enabled | disabled]
    adaptive-divergence-type [relative | absolute]
    adaptive-divergence-value [integer]
    adaptive-limit [integer]
    adaptive-sampling-timespan [integer]
    app-service [[string] | none]
    cert [ [cert list] | none]
    cipherlist [string]
    compatibility [enabled | disabled]
    defaults-from [name]
    description [string]
    destination [ip address][port]
    interval [integer]
    ip-dscp [integer]
    key [ [key] | none]
    manual-resume [enabled | disabled]
    password [none | [password] ]
    recv [none | [string] ]
    recv-disable [none | [string] ]
    reverse [enabled | disabled]
    send [none | [string] ]
    time-until-up [integer]
    timeout [integer]
    transparent [enabled | disabled]
    up-interval [integer]
    username [ [name] | none]
edit https [ [ [name] | [glob] | [regex] ] ... ]
    all-properties
    non-default-properties
```

Display

```
list https
list https [ [ [name] | [glob] | [regex] ] ... ]
show https [ [ [name] | [glob] | [regex] ] ... ]
show running-config https
show running-config https [ [ [name] | [glob] | [regex] ] ... ]
    all-properties
    non-default-properties
    one-line
    partition
```

Delete

```
delete https [name]
```

◆ Note

You cannot delete default monitors.

Description

You can use the **https** component to configure a custom monitor, or you can use the default HTTPS monitor that the Local Traffic Manager provides. This type of monitor verifies the HTTPS service by attempting to receive specific content from a Web page protected by Secure Socket Layer (SSL) security.

Note that one of the pre-configured HTTPS monitors is named **https_443**, which performs a health check on a server using the IP address supplied by the pool member and port **443**.

Examples

create https my_https defaults-from https

Creates a monitor named **my_https** that inherits properties from the default HTTPS monitor.

list https

Displays the properties of all of the HTTPS monitors.

Options

- **adaptive**
  Specifies whether the adaptive feature is enabled for this monitor. Not all monitors support the adaptive feature.
- **adaptive-divergence-type**
  Specifies whether the *adaptive-divergence-value* is **relative** or **absolute**.
- **adaptive-divergence-value**
  Specifies how far from mean latency each monitor probe is allowed to be. If *adaptive-divergence-type* is *relative*, this value is a percentage deviation from mean (e.g. 50 would indicate the probe is allowed to exceed the mean latency by 50%.) If *adaptive-divergence-type* is *absolute*, this value is an offset from mean in milliseconds (e.g. 250 would indicate the probe is allowed allowed to exceed the mean latency by 250 ms.) A probe that exceeds latency is counted the same as a probe that is not received, so in the typical scenario, it will require three missed latencies in a row to mark a pool member or node down (i.e. a 15-second interval with a 46-second timeout, would require three missed probes before the pool member or node would be marked down.)

- **adaptive-limit**
  Specifies the hard limit, in milliseconds, which the probe is not allowed to exceed, regardless of the divergence value. For example, if this value is 500, then the probe latency may not exceed 500 ms even if that would still fall within the divergence value.
- **adaptive-sampling-timespan**
  Specifies the size of the sliding window, in seconds, which records probe history. For example, if this value is 300, then a sliding window of the last five minutes' probe history will be used for calculating probe mean latency and standard deviation.
- **app-service**
  Specifies the name of the application service to which the monitor belongs. The default value is **none**. **Note:** If the **strict-updates** option is **enabled** on the application service that owns the object, you cannot modify or delete the monitor. Only the application service can modify or delete the monitor.
- **cert**
  Specifies a file object for a client certificate that the monitor sends to the target SSL server. The default value is **none**.
- **cipherlist**
  Specifies the list of ciphers for this monitor. The default list **DEFAULT:+SHA:+3DES:+kEDH** is located in the file **base_monitors.conf**.
- **compatibility**
  Specifies, when enabled, that the SSL options setting (in OpenSSL) is set to ALL. The default value is **enabled**.
- **defaults-from**
  Specifies the name of the monitor from which you want your custom monitor to inherit settings. The default value is **https**.
- **description**
  User defined description.
- **destination**
  Specifies the IP address and service port of the resource that is the destination of this monitor. The default value is ***:***.
  Possible values are:
  - ***:***
    Specifies to perform a health check on the IP address and port supplied by a pool member.
  - ***:port**
    Specifies to perform a health check on the server with the IP address supplied by the pool member and the port you specify.
  - **IP address:port**
    Specifies to mark a pool member **up** or **down** based on the response of the server at the IP address and port you specify.

- **IP address:port** (with the **transparent** option **enabled**)
  Specifies to perform a health check on the server at the IP address and port specified in the monitor, routing the check through the IP address and port supplied by the pool member. The pool member (the gateway) is marked up or down accordingly.

- **glob**
  Displays the items that match the **glob** expression. See **help glob** for a description of **glob** expression syntax.

- **interval**
  Specifies, in seconds, the frequency at which the system issues the monitor check when either the resource is **down** or the status of the resource is unknown. The default value is **5** seconds.

Important

*F5 Networks recommends that when you configure this option and the **up-interval** option, whichever value is greater be a multiple of the lesser value to allow for an even distribution of monitor checks among all monitors.*

- **ip-dscp**
  Specifies the differentiated services code point (DSCP). DSCP is a 6-bit value in the Differentiated Services (DS) field of the IP header. It can be used to specify the quality of service desired for the packet. The valid range for this value is 0 to 63 (hex 0x0 to 0x3f). The default value is zero.

- **key**
  Specifies the RSA private key if the monitored target requires authentication. The key must be surrounded by quotation marks, for example, **key "client.key"**. Note that if you specify a key, you must also specify a value for the **cert** option. The default value is **none**.

- **manual-resume**
  Specifies whether the system automatically changes the status of a resource to **up** at the next successful monitor check. The default value of the manual-resume option is **disabled**.
  Note that if you set the **manual-resume** option to **enabled**, you must manually mark the resource as **up** before the system can use it for load balancing connections.

- **name**
  Specifies a unique name for the component. This option is required for the commands **create**, **delete**, and **modify**.

- **partition**
  Displays the administrative partition within which the component resides.

- **password**
  Specifies the password if the monitored target requires authentication. The default value is **none**.

- **recv**
  Specifies the text string that the monitor looks for in the returned resource. The default value is **none**.

The most common receive expressions contain a text string that is included in an HTML file on your site. The text string can be regular text, HTML tags, or image names, and the associated operation is not case-sensitive. If you do not specify a value for both the **send** and **recv** options, the monitor performs a simple service check and connect only.

- **recv-disable**
  Specifies a text string that the monitor looks for in the returned resource. If the text string is matched in the returned resource, the corresponding node or pool member is marked session disabled. The default value is **none**.
  You specify a **recv-disable** string in the same way that you specify a **recv** string.
  If you specify a **recv-disable** string, you must also specify a **recv** string.
  You cannot specify a **recv-disable** string, if the **reverse** option is **enabled**.
- **regex**
  Displays the items that match the regular expression. The regular expression must be preceded by an at sign (@[regular expression]) to indicate that the identifier is a regular expression. See **help regex** for a description of regular expression syntax.
- **reverse**
  Specifies whether the monitor operates in reverse mode. When the monitor is in reverse mode, a successful check marks the monitored object **down** instead of **up**. You can use the this mode only if you configure both the **send** and **recv** options.
  The default value is **disabled**, which specifies that the monitor does not operate in reverse mode. The **enabled** value specifies that the monitor operates in reverse mode.
- **send**
  Specifies the text string that the monitor sends to the target object.
  The default setting is **GET /**, which retrieves a default HTML file for a web site. To retrieve a specific page from a web site, specify a fully-qualified path name, for example, **GET /www/company/index.html**.
  Since the string may have special characters, the system may require that the string be enclosed with single quotation marks.
  If this value is null, then a valid connection suffices to determine that the service is **up**. In this case, the system does not need the **recv** option and ignores the option even if not null.
- **time-until-up**
  Specifies the amount of time, in seconds, after the first successful response before a node is marked **up**. A value of **0** (zero) causes a node to be marked **up** immediately after a valid response is received from the node. The default value is **0** (zero).
- **timeout**
  Specifies the number of seconds the target has in which to respond to the monitor request. The default value is **16** seconds.
  If the target responds within the set time period, it is considered **up**. If the target does not respond within the set time period, it is considered **down**.

Also, if the target responds with a RESET packet, the system immediately flags the target as **down** without waiting for the timeout interval to expire.

- **transparent**
  Specifies whether the monitor operates in transparent mode. Monitors in transparent mode can monitor pool members through firewalls. The default value is **disabled**.
- **up-interval**
  Specifies, in seconds, the frequency at which the system issues the monitor check when the resource is **up**. The default value is **0** (zero), which specifies that the system uses the value of the **interval** option whether the resource is **up** or **down**.

Important

*F5 Networks recommends that when you configure this option and the **interval** option, whichever value is greater be a multiple of the lesser value to allow for an even distribution of monitor checks among all monitors.*

- **username**
  Specifies the username, if the monitored target requires authentication. The default value is **none**.

See Also

create, *delete*, *edit*, glob, *list*, *modify*, regex, *show*, *tmsh*

icmp

Configures an Internet Control Message Protocol (ICMP) monitor.

Syntax

Configure the **icmp** component within the **ltm monitor** module using the syntax shown in the following sections.

Create/Modify

```
create icmp [name]
modify icmp [name]
    adaptive [enabled | disabled]
    adaptive-divergence-type [relative | absolute]
    adaptive-divergence-value [integer]
    adaptive-limit [integer]
    adaptive-sampling-timespan [integer]
    app-service [[string] | none]
    defaults-from [name]
    description [string]
    destination [ip address]
    interval [integer]
    manual-resume [enabled | disabled]
    time-until-up [integer]
    timeout [integer]
    transparent [enabled | disabled]
    up-interval [integer]
edit icmp [ [ [name] | [glob] | [regex] ] ... ]
      all-properties
      non-default-properties
```

Display

```
list icmp
list icmp [ [ [name] | [glob] | [regex] ] ... ]
show icmp [ [ [name] | [glob] | [regex] ] ... ]
show running-config icmp
show running-config icmp [ [ [name] | [glob] | [regex] ] ... ]
    all-properties
    non-default-properties
    one-line
    partition
```

Delete

```
delete icmp [name]
```

◆ Note

You cannot delete default monitors.

Description

You can use the **icmp** component to configure a custom monitor, or you can use the default ICMP monitor that the Local Traffic Manager provides.

Examples

create icmp my_icmp defaults-from icmp

Creates a monitor named **my_icmp** that inherits properties from the default ICMP monitor.

list icmp

Displays the properties of all of the ICMP monitors.

Options

- **adaptive**
  Specifies whether the adaptive feature is enabled for this monitor. Not all monitors support the adaptive feature.
- **adaptive-divergence-type**
  Specifies whether the *adaptive-divergence-value* is **relative** or **absolute**.
- **adaptive-divergence-value**
  Specifies how far from mean latency each monitor probe is allowed to be. If *adaptive-divergence-type* is *relative*, this value is a percentage deviation from mean (e.g. 50 would indicate the probe is allowed to exceed the mean latency by 50%.) If *adaptive-divergence-type* is *absolute*, this value is an offset from mean in milliseconds (e.g. 250 would indicate the probe is allowed allowed to exceed the mean latency by 250 ms.) A probe that exceeds latency is counted the same as a probe that is not received, so in the typical scenario, it will require three missed latencies in a row to mark a pool member or node down (i.e. a 15-second interval with a 46-second timeout, would require three missed probes before the pool member or node would be marked down.)
- **adaptive-limit**
  Specifies the hard limit, in milliseconds, which the probe is not allowed to exceed, regardless of the divergence value. For example, if this value is 500, then the probe latency may not exceed 500 ms even if that would still fall within the divergence value.
- **adaptive-sampling-timespan**
  Specifies the size of the sliding window, in seconds, which records probe history. For example, if this value is 300, then a sliding window of the last five minutes' probe history will be used for calculating probe mean latency and standard deviation.
- **app-service**
  Specifies the name of the application service to which the monitor belongs. The default value is **none**. **Note:** If the **strict-updates** option is

enabled on the application service that owns the object, you cannot modify or delete the monitor. Only the application service can modify or delete the monitor.

- **defaults-from**
  Specifies the name of the monitor from which you want your custom monitor to inherit settings. The default value is **icmp**.
- **description**
  User defined description.
- **destination**
  Specifies the IP address of the resource that is the destination of this monitor. The default value is *****.
  Possible values are:
  - *****
    Specifies to perform a health check on the IP address of the node.
  - **IP address**
    Specifies to perform a health check on the IP address that you specify, and mark the associated node **up** or **down** accordingly.
  - **IP address** (with the **transparent** option **enabled**)
    Specifies to perform a health check on the IP address that you specify, route the check through the IP address of the associated node, and mark the IP address of the associated node **up** or **down** accordingly.
- **glob**
  Displays the items that match the **glob** expression. See **help glob** for a description of **glob** expression syntax.
- **interval**
  Specifies, in seconds, the frequency at which the system issues the monitor check when either the resource is **down** or the status of the resource is unknown. The default value is **5** seconds.

Important

*F5 Networks recommends that when you configure this option and the **up-interval** option, whichever value is greater be a multiple of the lesser value to allow for an even distribution of monitor checks among all monitors.*

- **manual-resume**
  Specifies whether the system automatically changes the status of a resource to **up** at the next successful monitor check. The default value of the manual-resume option is **disabled**.
  Note that if you set the **manual-resume** option to **enabled**, you must manually mark the resource as **up** before the system can use it for load balancing connections.
- **name**
  Specifies a unique name for the component. This option is required for the commands **create**, **delete**, and **modify**.

- **partition**
  Displays the administrative partition within which the component resides.
- **regex**
  Displays the items that match the regular expression. The regular expression must be preceded by an at sign (@[regular expression]) to indicate that the identifier is a regular expression. See **help regex** for a description of regular expression syntax.
- **time-until-up**
  Specifies the amount of time, in seconds, after the first successful response before a node is marked **up**. A value of **0** (zero) causes a node to be marked **up** immediately after a valid response is received from the node. The default value is **0** (zero).
- **timeout**
  Specifies the number of seconds the target has in which to respond to the monitor request. The default value is **16** seconds.
  If the target responds within the set time period, it is considered **up**. If the target does not respond within the set time period, it is considered **down**. Also, if the target responds with a RESET packet, the system immediately flags the target as **down** without waiting for the timeout interval to expire.
- **transparent**
  Specifies whether the monitor operates in transparent mode. Monitors in transparent mode can monitor pool members through firewalls. The default value is **disabled**.
- **up-interval**
  Specifies, in seconds, the frequency at which the system issues the monitor check when the resource is **up**. The default value is **0** (zero), which specifies that the system uses the value of the **interval** option whether the resource is **up** or **down**.

Important

*F5 Networks recommends that when you configure this option and the **interval** option, whichever value is greater be a multiple of the lesser value to allow for an even distribution of monitor checks among all monitors.*

See Also

create, *delete*, *edit*, glob, *list*, *modify*, regex, *show*, *tmsh*

imap

Configures an Internet Message Access Protocol (IMAP) monitor.

Syntax

Configure the **imap** component within the **ltm monitor** module using the syntax in the following sections.

Create/Modify

```
create imap [name]
modify imap [name]
    app-service [[string] | none]
    debug [no | yes]
    defaults-from [name]
    description [string]
    destination [ip address][port]
    folder [ [name] | none]
    interval [integer]
    manual-resume [enabled | disabled]
    password [none | [password] ]
    time-until-up [integer]
    timeout [integer]
    up-interval [integer]
    username [ [name] | none]
edit imap [ [ [name] | [glob] | [regex] ] ... ]
    all-properties
    non-default-properties
```

Display

```
list imap
list imap [ [ [name] | [glob] | [regex] ] ... ]
show imap [ [ [name] | [glob] | [regex] ] ... ]
show running-config imap
show running-config imap [ [ [name] | [glob] | [regex] ] ... ]
    all-properties
    non-default-properties
    one-line
    partition
```

Delete

```
delete imap [name]
```

◆ Note

You cannot delete default monitors.

Description

You can use the **imap** component to configure a custom monitor, or you can use the default IMAP monitor that the Local Traffic Manager provides. This type of monitor verifies IMAP by attempting to open a specified mail folder on a server. This monitor is similar to the POP3 monitor.

Examples

create imap my_imap defaults-from imap

Creates a monitor named **my_imap** that inherits properties from the default IMAP monitor.

list imap

Displays the properties of all of the IMAP monitors.

Options

- **app-service**
  Specifies the name of the application service to which the monitor belongs. The default value is **none**. **Note:** If the **strict-updates** option is **enabled** on the application service that owns the object, you cannot modify or delete the monitor. Only the application service can modify or delete the monitor.
- **debug**
  Specifies whether the monitor sends error messages and additional information to a log file created and labeled specifically for this monitor. You can use the log information to help diagnose and troubleshoot unsuccessful health checks.
  The default value is **no**. The options are:
  - **no**
    Specifies that the system does not redirect error messages and additional information related to this monitor.
  - **yes**
    Specifies that the system redirects error messages and additional information to the /var/log/monitors/<monitor_name>-<node_name>-<port>.log file.
- **defaults-from**
  Specifies the name of the monitor from which you want your custom monitor to inherit settings. The default value is **imap**.
- **description**
  User defined description.
- **destination**
  Specifies the IP address and service port of the resource that is the destination of this monitor. The default value is ***:***.
  Possible values are:

- ***:***
  Specifies to perform a health check on the IP address and port supplied by a pool member.
- ***:port**
  Specifies to perform a health check on the server with the IP address supplied by the pool member and the port you specify.
- **IP address:port**
  Specifies to mark a pool member **up** or **down** based on the response of the server at the IP address and port you specify.

◆ **folder**
Specifies the name of the folder on the IMAP server that the monitor tries to open. The default value is **INBOX**.

◆ **glob**
Displays the items that match the **glob** expression. See **help glob** for a description of **glob** expression syntax.

◆ **interval**
Specifies, in seconds, the frequency at which the system issues the monitor check when either the resource is **down** or the status of the resource is unknown. The default value is **10** seconds.

Important

*F5 Networks recommends that when you configure this option and the **up-interval** option, whichever value is greater be a multiple of the lesser value to allow for an even distribution of monitor checks among all monitors.*

◆ **manual-resume**
Specifies whether the system automatically changes the status of a resource to **up** at the next successful monitor check. The default value of the manual-resume option is **disabled**.
Note that if you set the **manual-resume** option to **enabled**, you must manually mark the resource as **up** before the system can use it for load balancing connections.

◆ **name**
Specifies a unique name for the component. This option is required for the commands **create**, **delete**, and **modify**.

◆ **partition**
Displays the administrative partition within which the component resides.

◆ **password**
Specifies the password if the monitored target requires authentication. The default value is **none**.

◆ **regex**
Displays the items that match the regular expression. The regular expression must be preceded by an at sign (@[regular expression]) to indicate that the identifier is a regular expression. See **help regex** for a description of regular expression syntax.

- **time-until-up**
  Specifies the amount of time, in seconds, after the first successful response before a node is marked **up**. A value of **0** (zero) causes a node to be marked **up** immediately after a valid response is received from the node. The default value is **0** (zero).
- **timeout**
  Specifies the number of seconds the target has in which to respond to the monitor request. The default value is **31** seconds.
  If the target responds within the set time period, it is considered **up**. If the target does not respond within the set time period, it is considered **down**. Also, if the target responds with a RESET packet, the system immediately flags the target as **down** without waiting for the timeout interval to expire.
- **up-interval**
  Specifies, in seconds, the frequency at which the system issues the monitor check when the resource is **up**. The default value is **0** (zero), which specifies that the system uses the value of the **interval** option whether the resource is **up** or **down**.

Important

*F5 Networks recommends that when you configure this option and the **interval** option, whichever value is greater be a multiple of the lesser value to allow for an even distribution of monitor checks among all monitors.*

- **username**
  Specifies the username, if the monitored target requires authentication. The default value is **none**.

See Also

create, *delete*, *edit*, glob, *list*, *modify*, regex, *show*, *tmsh*

inband

Configures an Inband (passive) monitor.

Syntax

Configure the **inband** component within the **ltm monitor** module using the syntax in the following sections.

Create/Modify

```
create inband [name]
modify inband [name]
    app-service [[string] | none]
    defaults-from [name]
    description [string]
    failure-interval [integer]
    failures [integer]
    response-time [integer]
    retry-time [integer]
edit inband [ [ [name] | [glob] | [regex] ] ... ]
    all-properties
    non-default-properties
```

Display

```
list inband
list inband [ [ [name] | [glob] | [regex] ] ... ]
show inband [ [ [name] | [glob] | [regex] ] ... ]
show running-config inband
show running-config inband [ [ [name] | [glob] | [regex] ] ... ]
    all-properties
    non-default-properties
    one-line
    partition
```

Delete

```
delete inband [name]
```

◆ Note

You cannot delete default monitors.

Description

You can use the **inband** component to configure a custom monitor, or you can use the default Inband monitor that the Local Traffic Manager provides. With this type of monitor the BIG-IP® system can perform passive monitoring as part of client requests.

Examples

create inband my_inband defaults-from inband

Creates a monitor named **my_inband** that inherits properties from the default Inband monitor.

list inband

Displays the properties of all of the Inband monitors.

Options

- **app-service**
  Specifies the name of the application service to which the monitor belongs. The default value is **none**. **Note:** If the **strict-updates** option is **enabled** on the application service that owns the object, you cannot modify or delete the monitor. Only the application service can modify or delete the monitor.
- **defaults-from**
  Specifies the name of the monitor from which you want your custom monitor to inherit settings. The default value is **inband**.
- **description**
  User defined description.
- **failure-interval**
  Specifies an interval, in seconds. If the number of failures specified in the **failures** option occurs within this interval, the system marks the pool member as being unavailable. The default value is **30**.
- **failures**
  Specifies the number of failures that the system allows to occur, within the time period specified in the **failure-interval** option, before marking a pool member unavailable. The default value is **3**, which means that the system marks the pool member unavailable at the fourth failure. The multiple tmm processes use a per-process number to calculate failures, depending on the specified load. For example, for the Round Robin load balancing method, if there are N tmm processes and M pool members, and the Failures setting is set to L, then up to N*M*L+1 failures can occur before the system marks the node as down.
  Specifying a value of **0** (zero) disables this option.
  A **failure** can be either a failure to connect or a failure of the pool member to respond within the time specified in the **response-time** option.
- **glob**
  Displays the items that match the **glob** expression. See **help glob** for a description of **glob** expression syntax.
- **name**
  Specifies a unique name for the component. This option is required for the commands **create**, **delete**, and **modify**.

- **partition**
  Displays the administrative partition within which the component resides.
- **regex**
  Displays the items that match the regular expression. The regular expression must be preceded by an at sign (@[regular expression]) to indicate that the identifier is a regular expression. See **help regex** for a description of regular expression syntax.
- **response-time**
  Specfies an amount of time, in seconds. If the pool member does not respond with data after the specified amount of time has passed, the number of failures in this interval increments by 1. Specifying a value of **0** (zero) disables this option.
- **retry-time**
  Specifies the amount of time in seconds after the pool member has been marked unavailable before the system retries to connect to the pool member. Specifying a value of **0** (zero) disables this option.

See Also

create, *delete*, *edit*, glob, *list*, *modify*, regex, *show*, *tmsh*

ldap

Configures a Lightweight Directory Access Protocol (LDAP) monitor.

Syntax

Configure the **ldap** component within the **ltm monitor** module using the syntax in the following sections.

Create/Modify

```
create ldap [name]
modify ldap [name]
    app-service [[string] | none]
    base [none | [string] ]
    chase-referrals [no | yes]
    debug [no | yes]
    defaults-from [name]
    description [string]
    destination [ip address][port]
    filter [ [LDAP key] | none]
    interval [integer]
    mandatory-attributes [no | yes]
    manual-resume [enabled | disabled]
    password [none | [password] ]
    security [none | ssl | tls]
    time-until-up [integer]
    timeout [integer]
    up-interval [integer]
    username [ [name] | none]
edit ldap [ [ [name] | [glob] | [regex] ] ... ]
    all-properties
    non-default-properties
```

Display

```
list ldap
list ldap [ [ [name] | [glob] | [regex] ] ... ]
show ldap [ [ [name] | [glob] | [regex] ] ... ]
show running-config ldap
show running-config ldap [ [ [name] | [glob] | [regex] ] ... ]
    all-properties
    non-default-properties
    one-line
    partition
```

Delete

```
delete ldap [name]
```

◆ Note

You cannot delete default monitors.

Description

You can use the **ldap** component to configure a custom monitor, or you can use the default LDAP monitor that the Local Traffic Manager provides. This type of monitor verifies the LDAP service by attempting to authenticate the specified user.

Examples

create ldap my_ldap defaults-from ldap

Creates a monitor named **my_ldap** that inherits properties from the default LDAP monitor.

list ldap

Displays the properties of all of the LDAP monitors.

Options

- **app-service**
  Specifies the name of the application service to which the monitor belongs. The default value is **none**. **Note:** If the **strict-updates** option is **enabled** on the application service that owns the object, you cannot modify or delete the monitor. Only the application service can modify or delete the monitor.
- **base**
  Specifies the location in the LDAP tree from which the monitor starts the health check. A sample value is **dc=bigip-test,dc=net**. The default value is **none**.
- **chase-referrals**
  Specifies whether the monitor upon receipt of an LDAP referral entry chases that referral. The default value is **yes**.
  The options are:
  - **no**
    Specifies that the system will treat a referral entry as a normal entry and refrain from querying the remote LDAP server(s) pointed to by the referral entry.
  - **yes**
    Specifies that the system upon receiving any referral entry from the monitored LDAP server query, the system will then query the corresponding LDAP server(s) pointed to by the LDAP query. If the query for the referral is unsuccessful the system will mark the monitored LDAP server down.
- **debug**
  Specifies whether the monitor sends error messages and additional information to a log file created and labeled specifically for this monitor.

You can use the log information to help diagnose and troubleshoot unsuccessful health checks. The default value is **no**.
The options are:

- **no**
  Specifies that the system does not redirect error messages and additional information related to this monitor.
- **yes**
  Specifies that the system redirects error messages and additional information to the /var/log/monitors/<monitor_name>-<node_name>-<port>.log file.

- **defaults-from**
  Specifies the name of the monitor from which you want your custom monitor to inherit settings. The default value is **ldap**.
- **description**
  User defined description.
- **destination**
  Specifies the IP address and service port of the resource that is the destination of this monitor. The default value is ***:***.
  Possible values are:
  - ***:***
    Specifies to perform a health check on the address and port supplied by a pool member.
  - ***:port**
    Specifies to perform a health check on the server with the IP address supplied by the pool member and the port you specify.
  - **IP address:port**
    Specifies to mark a pool member **up** or **down** based on the response of the server at the IP address and port you specify.
- **filter**
  Specifies an LDAP key for which the monitor searches. A sample value is **objectclass=***. The default value is **none**.
- **glob**
  Displays the items that match the **glob** expression. See **help glob** for a description of **glob** expression syntax.
- **interval**
  Specifies, in seconds, the frequency at which the system issues the monitor check when either the resource is **down** or the status of the resource is unknown. The default value is **10** seconds.

Important

*F5 Networks recommends that when you configure this option and the **up-interval** option, whichever value is greater be a multiple of the lesser value to allow for an even distribution of monitor checks among all monitors.*

- **mandatory-attributes**
  Specifies whether the target must include attributes in its response to be considered **up**. The default value is **no**.
  The options are:
  - **no**
    Specifies that the system performs only a one-level search (based on the value of the **filter** option), and does not require that the target returns any attributes.
  - **yes**
    Specifies that the system performs a sub-tree search, and if the target returns no attributes, the target is considered **down**.
- **manual-resume**
  Specifies whether the system automatically changes the status of a resource to **up** at the next successful monitor check. The default value of the manual-resume option is **disabled**.
  Note that if you set the **manual-resume** option to **enabled**, you must manually mark the resource as **up** before the system can use it for load balancing connections.
- **name**
  Specifies a unique name for the component. This option is required for the commands **create**, **delete**, and **modify**.
- **partition**
  Displays the administrative partition within which the component resides.
- **password**
  Specifies the password if the monitored target requires authentication. The default value is **none**.
- **regex**
  Displays the items that match the regular expression. The regular expression must be preceded by an at sign (@[regular expression]) to indicate that the identifier is a regular expression. See **help regex** for a description of regular expression syntax.
- **security**
  Specifies the secure communications protocol that the monitor uses to communicate with the target. The default value is **none**. The options are:
  - **none**
    Specifies that the system does not use a security protocol for communications with the target.
  - **ssl**
    Specifies that the system uses the SSL protocol for communications with the target.
  - **tls**
    Specifies that the system uses the TLS protocol for communications with the target.

- **time-until-up**
  Specifies the amount of time, in seconds, after the first successful response before a node is marked **up**. A value of **0** (zero) causes a node to be marked **up** immediately after a valid response is received from the node. The default value is **0** (zero).
- **timeout**
  Specifies the number of seconds the target has in which to respond to the monitor request. The default value is **31** seconds.
  If the target responds within the set time period, it is considered **up**. If the target does not respond within the set time period, it is considered **down**. Also, if the target responds with a RESET packet, the system immediately flags the target as **down** without waiting for the timeout interval to expire.
- **up-interval**
  Specifies, in seconds, the frequency at which the system issues the monitor check when the resource is **up**. The default value is **0** (zero), which specifies that the system uses the value of the **interval** option whether the resource is **up** or **down**.

Important

*F5 Networks recommends that when you configure this option and the **interval** option, whichever value is greater be a multiple of the lesser value to allow for an even distribution of monitor checks among all monitors.*

- **username**
  Specifies the username, if the monitored target requires authentication. The default value is **none**.

See Also

create, *delete*, *edit*, glob, *list*, *modify*, regex, *show*, *tmsh*

module-score

Configures a Module Score monitor that monitors the performance of a pool or node, rather than the health of the pool or node.

Syntax

Configure the **module-score** component within the **ltm monitor** module using the syntax in the following sections.

Create/Modify

```
create module-score [name]
modify module-score [name]
    app-service [[string] | none]
    debug [no | yes]
    defaults-from [name]
    description [string]
    interval [integer]
    pool [name]
    snmp-community [none | [string] ]
    snmp-ip-address [ [ip address] | none]
    snmp-port [port]
    snmp-version [string]
    time-until-up [integer]
    timeout [integer]
    up-interval [integer]
edit module-score [ [ [name] | [glob] | [regex] ] ... ]
    all-properties
    non-default-properties
```

Display

```
list module-score
list module-score [ [ [name] | [glob] | [regex] ] ... ]
show module-score [ [ [name] | [glob] | [regex] ] ... ]
show running-config module-score
show running-config module-score [ [ [name] | [glob] | [regex] ] ... ]
    all-properties
    non-default-properties
    one-line
    partition
```

Delete

```
delete module-score [name]
```

◆ Note

You cannot delete default monitors.

Description

You can use the **module-score** component to configure a custom monitor, or you can use the default Module Score monitor that the Local Traffic Manager provides. This type of monitor enables global and local traffic management systems to load balance in a proportional manner to local traffic management virtual servers associated with the Web Accelerator™ and Application Security Manager modules. When you configure a Module Score type of monitor, the local traffic management system uses SNMP to pull the gtm_score values from the downstream virtual servers and set the dynamic ratios on the associated upstream local traffic management pool members or nodes.

More specifically, the Module Score monitor retrieves the gtm_score values from the virtual server and the gtm_vs_score values associated with the virtual server. Then, if a pool name is not specified, this monitor sets the dynamic ratio on the node that is associated with the virtual server.

The BIG-IP® system uses the lowest non-zero value of the gtm_vs_score values to set the dynamic ratio. If all gtm_vs_score values are zero, then the gtm_score value is used to set the dynamic ratios. If you specify a pool name in the monitor definition, then the dynamic ratio is set on the pool member.

◆ Note

If you want to distribute traffic to a cluster of WebAccelerator or Application Security Manager virtual servers, you must create a separate custom Module Score monitor for each back-end Local Traffic Manager system.

Examples

create module-score my_module-score defaults-from module_score

Creates a monitor named **my_module-score** that inherits properties from the default Module Score monitor.

list module-score

Displays the properties of all of the Module Score monitors.

Options

- **app-service**
  Specifies the name of the application service to which the monitor belongs. The default value is **none**. **Note:** If the **strict-updates** option is **enabled** on the application service that owns the object, you cannot modify or delete the monitor. Only the application service can modify or delete the monitor.

- **debug**
  Specifies whether the monitor sends error messages and additional information to a log file created and labeled specifically for this monitor. You can use the log information to help diagnose and troubleshoot unsuccessful health checks. The default value is **no**.
  The options are:
  - **no**
    Specifies that the system does not redirect error messages and additional information related to this monitor.
  - **yes**
    Specifies that the system redirects error messages and additional information to the /var/log/monitors/<monitor_name>-<node_name>-<port>.log file.
- **defaults-from**
  Specifies the name of the monitor from which you want your custom monitor to inherit settings. The default value is **module_score**.
- **description**
  User defined description.
- **glob**
  Displays the items that match the **glob** expression. See **help glob** for a description of **glob** expression syntax.
- **interval**
  Specifies, in seconds, the frequency at which the system issues the monitor check when either the resource is **down** or the status of the resource is unknown. The default value is **10** seconds.

Important

*F5 Networks recommends that when you configure this option and the **up-interval** option, whichever value is greater be a multiple of the lesser value to allow for an even distribution of monitor checks among all monitors.*

- **name**
  Specifies a unique name for the component. This option is required for the commands **create**, **delete**, and **modify**.
- **partition**
  Displays the administrative partition within which the component resides.
- **pool**
  Specifies a Local Traffic Manager pool name. Use this option if you want the system to set dynamic ratios on a pool member instead of on the associated node for the pool member. The default value is **none**.
- **regex**
  Displays the items that match the regular expression. The regular expression must be preceded by an at sign (@[regular expression]) to indicate that the identifier is a regular expression. See **help regex** for a description of regular expression syntax.

- **snmp-community**
  Specifies the identifier for the SNMP community. The default value is **public**.
- **snmp-ip-address**
  Specifies the IP address of the SNMP server. The default value is **none**.
- **snmp-port**
  Specifies the port associated with the SNMP server. The default value is **161**.
- **snmp-version**
  Specifies the SNMP version in use by the system. The default value is **v2c**.
- **time-until-up**
  Specifies the amount of time in seconds after the first successful response before a node is marked up. A value of **0** (zero) causes a node to be marked up immediately after a valid response is received from the node. The default value is **0** (zero).
- **timeout**
  Specifies the number of seconds the target has in which to respond to the monitor request. The default value is **30** seconds.
  If the target responds within the set time period, it is considered **up**. If the target does not respond within the set time period, it is considered **down**. Also, if the target responds with a RESET packet, the system immediately flags the target as **down** without waiting for the timeout interval to expire.
- **up-interval**
  Specifies, in seconds, the frequency at which the system issues the monitor check when the resource is **up**. The default value is **0** (zero), which specifies that the system uses the value of the **interval** option whether the resource is **up** or **down**.

Important

*F5 Networks recommends that when you configure this option and the **interval** option, whichever value is greater be a multiple of the lesser value to allow for an even distribution of monitor checks among all monitors.*

See Also

create, *delete*, *edit*, glob, *list*, *modify*, regex, *show*, *tmsh*

mssql

Configures a Microsoft® Windows® Structured Query Language (MSSQL) monitor.

Syntax

Configure the **mssql** component within the **ltm monitor** module using the syntax in the following sections.

Create/Modify

```
create mssql [name]
modify mssql [name]
    app-service [[string] | none]
    count [integer]
    database [ [name] | none]
    debug [no | yes]
    defaults-from [name]
    description [string]
    destination [ip address][port]
    interval [integer]
    manual-resume [enabled | disabled]
    password [none | [password] ]
    recv [none | [string] ]
    recv-column [none | [string] ]
    recv-row [none | [string] ]
    send [none | [string] ]
    time-until-up [integer]
    timeout [integer]
    up-interval [integer]
    username [[name] | none]
edit mssql [ [ [name] | [glob] | [regex] ] ... ]
    all-properties
    non-default-properties
```

Display

```
list mssql
list mssql [ [ [name] | [glob] | [regex] ] ... ]
show mssql [ [ [name] | [glob] | [regex] ] ... ]
show running-config mssql
show running-config mssql [ [ [name] | [glob] | [regex] ] ... ]
    all-properties
    non-default-properties
    one-line
    partition
```

Delete

```
delete mssql [name]
```

◆ Note

You cannot delete default monitors.

Description

You can use the **mssql** component to configure a custom monitor, or you can use the default Microsoft Windows SQL monitor that the Local Traffic Manager provides. This type of monitor verifies Microsoft Windows SQL-based services.

Examples

create mssql my_mssql defaults-from mssql

Creates a monitor named **my_mssql** that inherits properties from the default MSSQL monitor.

list mssql

Displays the properties of all of the MSSQL monitors.

Options

- **app-service**
  Specifies the name of the application service to which the monitor belongs. The default value is **none**. **Note:** If the **strict-updates** option is **enabled** on the application service that owns the object, you cannot modify or delete the monitor. Only the application service can modify or delete the monitor.
- **count**
  Specifies the number of monitor probes after which the connection to the database will be terminated. Count value of zero indicates that the connection will never be terminated. The default value is **zero**.
- **database**
  Specifies the name of the database with which the monitor attempts to communicate. The default value is **none**.
- **debug**
  Specifies whether the monitor sends error messages and additional information to a log file created and labeled specifically for this monitor. You can use the log information to help diagnose and troubleshoot unsuccessful health checks. The default value is **no**.
  The options are:
  - **no**
    Specifies that the system does not redirect error messages and additional information related to this monitor.
  - **yes**
    Specifies that the system redirects error messages and additional information to the /var/log/monitors/<monitor_name>-<node_name>-<port>.log file.
- **defaults-from**
  Specifies the name of the monitor from which you want your custom monitor to inherit settings. The default value is **mssql**.

- **description**
  User defined description.
- **destination**
  Specifies the IP address and service port of the resource that is the destination of this monitor. The default value is ***:***.
  Possible values are:
  - ***:***
    Specifies to perform a health check on the IP address and port supplied by a pool member.
  - ***:port**
    Specifies to perform a health check on the server with the IP address supplied by the pool member and the port you specify.
  - **IP address:port**
    Specifies to mark a pool member **up** or **down** based on the response of the server at the IP address and port you specify.
- **glob**
  Displays the items that match the **glob** expression. See **help glob** for a description of **glob** expression syntax.
- **interval**
  Specifies, in seconds, the frequency at which the system issues the monitor check when either the resource is **down** or the status of the resource is unknown. The default value is **30** seconds.

Important

*F5 Networks recommends that when you configure this option and the **up-interval** option, whichever value is greater be a multiple of the lesser value to allow for an even distribution of monitor checks among all monitors.*

- **manual-resume**
  Specifies whether the system automatically changes the status of a resource to **up** at the next successful monitor check. The default value of the manual-resume option is **disabled**.
  Note that if you set the **manual-resume** option to **enabled**, you must manually mark the resource as **up** before the system can use it for load balancing connections.
- **name**
  Specifies a unique name for the component. This option is required for the commands **create**, **delete**, and **modify**.
- **partition**
  Displays the administrative partition within which the component resides.
- **password**
  Specifies the password if the monitored target requires authentication. The default value is **none**.

- **recv**
  Specifies the text string that the monitor looks for in the returned resource. The default value is **none**.
  The most common receive expressions contain a text string that is included in a field in your database. If you do not specify a value for both the **send** and **recv** options, the monitor performs a simple service check and connect only.
- **recv-column**
  Specifies the column in the database where the system expects the specified Receive String to be located. Specify this option only if you configure the **send** and **recv** options. The default value is **none**.
- **recv-row**
  Specifies the row in the database where the system expects the specified Receive String to be located. Specify this option only if you configure the **send** and **recv** options. The default value is **none**.
- **regex**
  Displays the items that match the regular expression. The regular expression must be preceded by an at sign (@[regular expression]) to indicate that the identifier is a regular expression. See **help regex** for a description of regular expression syntax.
- **send**
  Specifies the SQL query that the monitor sends to the target database, for example, **SELECT count(*) FROM mytable**.
  If this value is null, then a valid connection suffices to determine that the service is **up**. In this case, the system does not need the recv option and ignores the option even if not null.
- **time-until-up**
  Specifies the amount of time, in seconds, after the first successful response before a node is marked **up**. A value of **0** (zero) causes a node to be marked **up** immediately after a valid response is received from the node. The default value is **0** (zero).
- **timeout**
  Specifies the number of seconds the target has in which to respond to the monitor request. The default value is **91** seconds.
  If the target responds within the set time period, it is considered **up**. If the target does not respond within the set time period, it is considered **down**. Also, if the target responds with a RESET packet, the system immediately flags the target as **down** without waiting for the timeout interval to expire.

- **up-interval**
  Specifies, in seconds, the frequency at which the system issues the monitor check when the resource is **up**. The default value is **0** (zero), which specifies that the system uses the value of the **interval** option whether the resource is **up** or **down**.

Important

*F5 Networks recommends that when you configure this option and the **interval** option, whichever value is greater be a multiple of the lesser value to allow for an even distribution of monitor checks among all monitors.*

- **username**
  Specifies the username, if the monitored target requires authentication. The default value is **none**.

See Also

create, *delete*, *edit*, glob, *list*, *modify*, regex, *show*, *tmsh*

mysql

Configures a MySQL® monitor.

Syntax

Configure the **mysql** component within the **ltm monitor** module using the syntax in the following sections.

Create/Modify

```
create mysql [name]
modify mysql [name]
    app-service [[string] | none]
    count [integer]
    database [ [name] | none]
    debug [no | yes]
    defaults-from [name]
    description [string]
    destination [ip address][port]
    interval [integer]
    manual-resume [enabled | disabled]
    password [none | [password] ]
    recv [none | [string] ]
    recv-column [none | [string] ]
    recv-row [none | [string] ]
    send [none | [string] ]
    time-until-up [integer]
    timeout [integer]
    up-interval [integer]
    username [[name] | none]
edit mysql [ [ [name] | [glob] | [regex] ] ... ]
    all-properties
    non-default-properties
```

Display

```
list mysql
list mysql [ [ [name] | [glob] | [regex] ] ... ]
show mysql [ [ [name] | [glob] | [regex] ] ... ]
show running-config mysql
show running-config mysql [ [ [name] | [glob] | [regex] ] ... ]
    all-properties
    non-default-properties
    one-line
    partition
```

Delete

```
delete mysql [name]
```

◆ Note

You cannot delete default monitors.

Description

You can use the **mysql** component to configure a custom monitor, or you can use the default MySQL monitor that the Local Traffic Manager provides. This type of monitor verifies MySQL-based services.

Examples

create mysql my_mysql defaults-from mysql

Creates a monitor named **my_mysql** that inherits properties from the default MySQL monitor.

list mysql

Displays the properties of all of the MySQL monitors.

Options

- **app-service**
  Specifies the name of the application service to which the monitor belongs. The default value is **none**. **Note:** If the **strict-updates** option is **enabled** on the application service that owns the object, you cannot modify or delete the monitor. Only the application service can modify or delete the monitor.
- **count**
  Specifies the number of monitor probes after which the connection to the database will be terminated. Count value of zero indicates that the connection will never be terminated. The default value is **zero**.
- **database**
  Specifies the name of the database with which the monitor attempts to communicate. The default value is **none**.
- **debug**
  Specifies whether the monitor sends error messages and additional information to a log file created and labeled specifically for this monitor. You can use the log information to help diagnose and troubleshoot unsuccessful health checks. The default value is **no**.
  The options are:
  - **no**
    Specifies that the system does not redirect error messages and additional information related to this monitor.
  - **yes**
    Specifies that the system redirects error messages and additional information to the /var/log/monitors/<monitor_name>-<node_name>-<port>.log file.
- **defaults-from**
  Specifies the name of the monitor from which you want your custom monitor to inherit settings. The default value is **mysql**.

- **description**
  User defined description.
- **destination**
  Specifies the IP address and service port of the resource that is the destination of this monitor. The default value is ***:***.
  Possible values are:
  - ***:***
    Specifies to perform a health check on the IP address and port supplied by a pool member.
  - ***:port**
    Specifies to perform a health check on the server with the IP address supplied by the pool member and the port you specify.
  - **IP address:port**
    Specifies to mark a pool member **up** or **down** based on the response of the server at the IP address and port you specify.
- **glob**
  Displays the items that match the **glob** expression. See **help glob** for a description of **glob** expression syntax.
- **interval**
  Specifies, in seconds, the frequency at which the system issues the monitor check when either the resource is **down** or the status of the resource is unknown. The default value is **30** seconds.

Important

*F5 Networks recommends that when you configure this option and the **up-interval** option, whichever value is greater be a multiple of the lesser value to allow for an even distribution of monitor checks among all monitors.*

- **manual-resume**
  Specifies whether the system automatically changes the status of a resource to **up** at the next successful monitor check. The default value of the manual-resume option is **disabled**.
  Note that if you set the **manual-resume** option to **enabled**, you must manually mark the resource as **up** before the system can use it for load balancing connections.
- **name**
  Specifies a unique name for the component. This option is required for the commands **create**, **delete**, and **modify**.
- **partition**
  Displays the administrative partition within which the component resides.
- **password**
  Specifies the password if the monitored target requires authentication. The default value is **none**.

- **recv**
  Specifies the text string that the monitor looks for in the returned resource. The default value is **none**.
  The most common receive expressions contain a text string that is included in a field in your database. If you do not specify a value for both the **send** and **recv** options, the monitor performs a simple service check and connect only.
- **recv-column**
  Specifies the column in the database where the system expects the specified Receive String to be located. Specify this option only if you configure the **send** and **recv** options. The default value is **none**.
- **recv-row**
  Specifies the row in the database where the system expects the specified Receive String to be located. Specify this option only if you configure the **send** and **recv** options. The default value is **none**.
- **regex**
  Displays the items that match the regular expression. The regular expression must be preceded by an at sign (@[regular expression]) to indicate that the identifier is a regular expression. See **help regex** for a description of regular expression syntax.
- **send**
  Specifies the SQL query that the monitor sends to the target database, for example, **SELECT count(*) FROM mytable**.
  If this value is null, then a valid connection suffices to determine that the service is **up**. In this case, the system does not need the recv option and ignores the option even if not null.
- **time-until-up**
  Specifies the amount of time, in seconds, after the first successful response before a node is marked **up**. A value of **0** (zero) causes a node to be marked **up** immediately after a valid response is received from the node. The default value is **0** (zero).
- **timeout**
  Specifies the number of seconds the target has in which to respond to the monitor request. The default value is **91** seconds.
  If the target responds within the set time period, it is considered **up**. If the target does not respond within the set time period, it is considered **down**. Also, if the target responds with a RESET packet, the system immediately flags the target as **down** without waiting for the timeout interval to expire.

- **up-interval**
  Specifies, in seconds, the frequency at which the system issues the monitor check when the resource is **up**. The default value is **0** (zero), which specifies that the system uses the value of the **interval** option whether the resource is **up** or **down**.

Important

*F5 Networks recommends that when you configure this option and the **interval** option, whichever value is greater be a multiple of the lesser value to allow for an even distribution of monitor checks among all monitors.*

- **username**
  Specifies the username, if the monitored target requires authentication. The default value is **none**.

See Also

create, *delete*, *edit*, glob, *list*, *modify*, regex, *show*, *tmsh*

nntp

Configures a Network News Transfer Protocol (NNTP) monitor.

Syntax

Configure the **nntp** component within the **ltm monitor** module using the syntax in the following sections.

Create/Modify

```
create nntp [name]
modify nntp [name]
    app-service [[string] | none]
    debug [no | yes]
    defaults-from [name]
    description [string]
    destination [ip address][port]
    interval [integer]
    manual-resume [enabled | disabled]
    newsgroup [ [name] | none]
    password [none | [password] ]
    time-until-up [integer]
    timeout [integer]
    up-interval [integer]
    username [[name] | none]
edit nntp [ [ [name] | [glob] | [regex] ] ... ]
    all-properties
    non-default-properties
```

Display

```
list nntp
list nntp [ [ [name] | [glob] | [regex] ] ... ]
show nntp [ [ [name] | [glob] | [regex] ] ... ]
show running-config nntp
show running-config nntp [ [ [name] | [glob] | [regex] ] ... ]
    all-properties
    non-default-properties
    one-line
    partition
```

Delete

```
delete nntp [name]
```

◆ Note

You cannot delete default monitors.

Description

You can use the **nntp** component to configure a custom monitor, or you can use the default NNTP monitor that the Local Traffic Manager provides. This type of monitor verifies the Usenet News protocol service by attempting to retrieve a newsgroup identification string from the server.

Examples

create nntp my_nntp defaults-from nntp

Creates a monitor named **my_nntp** that inherits properties from the default NNTP monitor.

list nntp

Displays the properties of all of the NNTP monitors.

Options

- **app-service**
  Specifies the name of the application service to which the monitor belongs. The default value is **none**. **Note:** If the **strict-updates** option is **enabled** on the application service that owns the object, you cannot modify or delete the monitor. Only the application service can modify or delete the monitor.
- **debug**
  Specifies whether the monitor sends error messages and additional information to a log file created and labeled specifically for this monitor. You can use the log information to help diagnose and troubleshoot unsuccessful health checks. The default value is **no**.
  The options are:
  - **no**
    Specifies that the system does not redirect error messages and additional information related to this monitor.
  - **yes**
    Specifies that the system redirects error messages and additional information to the /var/log/monitors/<monitor_name>-<node_name>-<port>.log file.
- **defaults-from**
  Specifies the name of the monitor from which you want your custom monitor to inherit settings. The default value is **nntp**.
- **description**
  User defined description.
- **destination**
  Specifies the IP address and service port of the resource that is the destination of this monitor. The default value is ***:***.
  Possible values are:

- ***:***
  Specifies to perform a health check on the IP address and port supplied by a pool member.
- ***:port**
  Specifies to perform a health check on the server with the IP address supplied by the pool member and the port you specify.
- **IP address:port**
  Specifies to mark a pool member **up** or **down** based on the response of the server at the IP address and port you specify.

◆ **glob**
Displays the items that match the **glob** expression. See **help glob** for a description of **glob** expression syntax.

◆ **interval**
Specifies, in seconds, the frequency at which the system issues the monitor check when either the resource is **down** or the status of the resource is unknown. The default value is **5** seconds.

Important

*F5 Networks recommends that when you configure this option and the **up-interval** option, whichever value is greater be a multiple of the lesser value to allow for an even distribution of monitor checks among all monitors.*

◆ **manual-resume**
Specifies whether the system automatically changes the status of a resource to **up** at the next successful monitor check. The default value of the manual-resume option is **disabled**.
Note that if you set the **manual-resume** option to **enabled**, you must manually mark the resource as **up** before the system can use it for load balancing connections.

◆ **name**
Specifies a unique name for the component. This option is required for the commands **create**, **delete**, and **modify**.

◆ **newsgroup**
Specifies the name of the newsgroup that you are monitoring, for example **alt.car.mercedes**. The default value is **none**.

◆ **partition**
Displays the administrative partition within which the component resides.

◆ **password**
Specifies the password if the monitored target requires authentication. The default value is **none**.

◆ **regex**
Displays the items that match the regular expression. The regular expression must be preceded by an at sign (@[regular expression]) to indicate that the identifier is a regular expression. See **help regex** for a description of regular expression syntax.

- **time-until-up**
  Specifies the amount of time, in seconds, after the first successful response before a node is marked **up**. A value of **0** (zero) causes a node to be marked **up** immediately after a valid response is received from the node. The default value is **0** (zero).
- **timeout**
  Specifies the number of seconds the target has in which to respond to the monitor request. The default value is **16** seconds.
  If the target responds within the set time period, it is considered **up**. If the target does not respond within the set time period, it is considered **down**. Also, if the target responds with a RESET packet, the system immediately flags the target as **down** without waiting for the timeout interval to expire.
- **up-interval**
  Specifies, in seconds, the frequency at which the system issues the monitor check when the resource is **up**. The default value is **0** (zero), which specifies that the system uses the value of the **interval** option whether the resource is **up** or **down**.

Important

*F5 Networks recommends that when you configure this option and the **interval** option, whichever value is greater be a multiple of the lesser value to allow for an even distribution of monitor checks among all monitors.*

- **username**
  Specifies the username, if the monitored target requires authentication. The default value is **none**.

See Also

create, *delete*, *edit*, glob, *list*, *modify*, regex, *show*, *tmsh*

oracle

Configures an Oracle® monitor.

Syntax

Configure the **oracle** component within the **ltm monitor** module using the syntax in the following sections.

Create/Modify

```
create oracle [name]
modify oracle [name]
    app-service [[string] | none]
    count [integer]
    database [ [name] | none]
    debug [no | yes]
    defaults-from [name]
    description [string]
    destination [ip address][port]
    interval [integer]
    manual-resume [enabled | disabled]
    password [none | [password] ]
    recv [none | [string] ]
    recv-column [none | [string] ]
    recv-row [none | [string] ]
    send [none | [string] ]
    time-until-up [integer]
    timeout [integer]
    up-interval [integer]
    username [ [name] | none]
edit oracle [ [ [name] | [glob] | [regex] ] ... ]
    all-properties
    non-default-properties
```

Display

```
list oracle
list oracle [ [ [name] | [glob] | [regex] ] ... ]
show oracle [ [ [name] | [glob] | [regex] ] ... ]
show running-config oracle
show running-config oracle [ [ [name] | [glob] | [regex] ] ... ]
    all-properties
    non-default-properties
    one-line
    partition
```

Delete

```
delete oracle [name]
```

◆ Note

You cannot delete default monitors.

Description

You can use the **oracle** component to configure a custom monitor, or you can use the default Oracle monitor that the Local Traffic Manager provides. This type of monitor verifies Oracle database services.

Examples

create oracle my_oracle defaults-from oracle

Creates a monitor named **my_oracle** that inherits properties from the default Oracle monitor.

list oracle

Displays the properties of all of the Oracle monitors.

Options

- **app-service**
  Specifies the name of the application service to which the monitor belongs. The default value is **none**. **Note:** If the **strict-updates** option is **enabled** on the application service that owns the object, you cannot modify or delete the monitor. Only the application service can modify or delete the monitor.
- **count**
  Specifies the number of monitor probes after which the connection to the database will be terminated. Count value of zero indicates that the connection will never be terminated. The default value is **zero**.
- **database**
  Specifies the name of the database with which the monitor attempts to communicate. The proper format for database name is <node_ip>:<node_port>:<database_name>. The default value is **none**.
- **debug**
  Specifies whether the monitor sends error messages and additional information to a log file created and labeled specifically for this monitor. You can use the log information to help diagnose and troubleshoot unsuccessful health checks. The default value is **no**.
  The options are:
  - **no**
    Specifies that the system does not redirect error messages and additional information related to this monitor.
  - **yes**
    Specifies that the system redirects error messages and additional information to the /var/log/monitors/<monitor_name>-<node_name>-<port>.log file.
- **defaults-from**
  Specifies the name of the monitor from which you want your custom monitor to inherit settings. The default value is **oracle**.

- **description**
  User defined description.
- **destination**
  Specifies the IP address and service port of the resource that is the destination of this monitor. The default value is ***:***.
  Possible values are:
  - ***:***
    Specifies to perform a health check on the IP address and port supplied by a pool member.
  - ***:port**
    Specifies to perform a health check on the server with the IP address supplied by the pool member and the port you specify.
  - **IP address:port**
    Specifies to mark a pool member **up** or **down** based on the response of the server at the IP address and port you specify.
- **glob**
  Displays the items that match the **glob** expression. See **help glob** for a description of **glob** expression syntax.
- **interval**
  Specifies, in seconds, the frequency at which the system issues the monitor check when either the resource is **down** or the status of the resource is unknown. The default value is **30** seconds.

Important

*F5 Networks recommends that when you configure this option and the **up-interval** option, whichever value is greater be a multiple of the lesser value to allow for an even distribution of monitor checks among all monitors.*

- **manual-resume**
  Specifies whether the system automatically changes the status of a resource to **up** at the next successful monitor check. The default value of the manual-resume option is **disabled**.
  Note that if you set the **manual-resume** option to **enabled**, you must manually mark the resource as **up** before the system can use it for load balancing connections.
- **name**
  Specifies a unique name for the component. This option is required for the commands **create**, **delete**, and **modify**.
- **partition**
  Displays the administrative partition within which the component resides.
- **password**
  Specifies the password if the monitored target requires authentication. The default value is **none**.

- **recv**
  Specifies the text string that the monitor looks for in the returned resource. The default value is **none**.
  The most common receive expressions contain a text string that is included in a field in your database. If you do not specify a value for both the **send** and **recv** options, the monitor performs a simple service check and connect only.
- **recv-column**
  Specifies the column in the database where the system expects the specified Receive String to be located. Specify this option only if you configure the **send** and **recv** options. The default value is **none**.
- **recv-row**
  Specifies the row in the database where the system expects the specified Receive String to be located. Specify this option only if you configure the **send** and **recv** options. The default value is **none**.
- **regex**
  Displays the items that match the regular expression. The regular expression must be preceded by an at sign (@[regular expression]) to indicate that the identifier is a regular expression. See **help regex** for a description of regular expression syntax.
- **send**
  Specifies the SQL query that the monitor sends to the target database, for example, **SELECT count(*) FROM mytable**.
  If this value is null, then a valid connection suffices to determine that the service is **up**. In this case, the system does not need the recv option and ignores the option even if not null.
- **time-until-up**
  Specifies the amount of time, in seconds, after the first successful response before a node is marked **up**. A value of **0** (zero) causes a node to be marked **up** immediately after a valid response is received from the node. The default value is **0** (zero).
- **timeout**
  Specifies the number of seconds the target has in which to respond to the monitor request. The default value is **91** seconds.
  If the target responds within the set time period, it is considered **up**. If the target does not respond within the set time period, it is considered **down**. Also, if the target responds with a RESET packet, the system immediately flags the target as **down** without waiting for the timeout interval to expire.

- **up-interval**
  Specifies, in seconds, the frequency at which the system issues the monitor check when the resource is **up**. The default value is **0** (zero), which specifies that the system uses the value of the **interval** option whether the resource is **up** or **down**.

Important

*F5 Networks recommends that when you configure this option and the **interval** option, whichever value is greater be a multiple of the lesser value to allow for an even distribution of monitor checks among all monitors.*

- **username**
  Specifies the username, if the monitored target requires authentication. The default value is **none**.

See Also

create, *delete*, *edit*, glob, *list*, *modify*, regex, *show*, *tmsh*

pop3

Configures a Post Office Protocol (POP3) monitor.

Syntax

Configure the **pop3** component within the **ltm monitor** module using the syntax in the following sections.

Create/Modify

```
create pop3 [name]
modify pop3 [name]
    app-service [[string] | none]
    debug [no | yes]
    defaults-from [name]
    description [string]
    destination [ip address][port]
    interval [integer]
    manual-resume [enabled | disabled]
    password [none | [password] ]
    time-until-up [integer]
    timeout [integer]
    up-interval [integer]
    username [ [name] | none]
edit pop3 [ [ [name] | [glob] | [regex] ] ... ]
      all-properties
     non-default-properties
```

Display

```
list pop3
list pop3 [ [ [name] | [glob] | [regex] ] ... ]
show pop3 [ [ [name] | [glob] | [regex] ] ... ]
show running-config pop3
show running-config pop3 [ [ [name] | [glob] | [regex] ] ... ]
    all-properties
    non-default-properties
    one-line
    partition
```

Delete

```
delete pop3 [name]
```

◆ Note

You cannot delete default monitors.

Description

You can use the **pop3** component to configure a custom monitor, or you can use the default POP3 monitor that the Local Traffic Manager provides. This type of monitor verifies the POP3 service by attempting to connect to a pool, pool member, or virtual server, log on as the specified user, and log off.

Examples

create pop3 my_pop3 defaults-from pop3

Creates a monitor named **my_pop3** that inherits properties from the default POP3 monitor.

list pop3

Displays the properties of all of the POP3 monitors.

Options

- **app-service**
  Specifies the name of the application service to which the monitor belongs. The default value is **none**. **Note:** If the **strict-updates** option is **enabled** on the application service that owns the object, you cannot modify or delete the monitor. Only the application service can modify or delete the monitor.
- **debug**
  Specifies whether the monitor sends error messages and additional information to a log file created and labeled specifically for this monitor. You can use the log information to help diagnose and troubleshoot unsuccessful health checks.
  The default value is **no**. The options are:
  - **no**
    Specifies that the system does not redirect error messages and additional information related to this monitor.
  - **yes**
    Specifies that the system redirects error messages and additional information to the /var/log/monitors/<monitor_name>-<node_name>-<port>.log file.
- **defaults-from**
  Specifies the name of the monitor from which you want your custom monitor to inherit settings. The default value is **pop3**.
- **description**
  User defined description.
- **destination**
  Specifies the IP address and service port of the resource that is the destination of this monitor. The default value is ***:***.
  Possible values are:

- ***:***
  Specifies to perform a health check on the IP address and port supplied by a pool member.
- ***:port**
  Specifies to perform a health check on the server with the IP address supplied by the pool member and the port you specify.
- **IP address:port**
  Specifies to mark a pool member **up** or **down** based on the response of the server at the IP address and port you specify.

◆ **glob**
Displays the items that match the **glob** expression. See **help glob** for a description of **glob** expression syntax.

◆ **interval**
Specifies, in seconds, the frequency at which the system issues the monitor check when either the resource is **down** or the status of the resource is unknown. The default value is **5** seconds.

Important

*F5 Networks recommends that when you configure this option and the **up-interval** option, whichever value is greater be a multiple of the lesser value to allow for an even distribution of monitor checks among all monitors.*

◆ **manual-resume**
Specifies whether the system automatically changes the status of a resource to **up** at the next successful monitor check. The default value of the manual-resume option is **disabled**.
Note that if you set the **manual-resume** option to **enabled**, you must manually mark the resource as **up** before the system can use it for load balancing connections.

◆ **name**
Specifies a unique name for the component. This option is required for the commands **create**, **delete**, and **modify**.

◆ **partition**
Displays the administrative partition within which the component resides.

◆ **password**
Specifies the password if the monitored target requires authentication. The default value is **none**.

◆ **regex**
Displays the items that match the regular expression. The regular expression must be preceded by an at sign (@[regular expression]) to indicate that the identifier is a regular expression. See **help regex** for a description of regular expression syntax.

- **time-until-up**
  Specifies the amount of time, in seconds, after the first successful response before a node is marked **up**. A value of **0** (zero) causes a node to be marked **up** immediately after a valid response is received from the node. The default value is **0** (zero).
- **timeout**
  Specifies the number of seconds the target has in which to respond to the monitor request. The default value is **16** seconds.
  If the target responds within the set time period, it is considered **up**. If the target does not respond within the set time period, it is considered **down**. Also, if the target responds with a RESET packet, the system immediately flags the target as **down** without waiting for the timeout interval to expire.
- **up-interval**
  Specifies, in seconds, the frequency at which the system issues the monitor check when the resource is **up**. The default value is **0** (zero), which specifies that the system uses the value of the **interval** option whether the resource is **up** or **down**.

Important

*F5 Networks recommends that when you configure this option and the **interval** option, whichever value is greater be a multiple of the lesser value to allow for an even distribution of monitor checks among all monitors.*

- **username**
  Specifies the username, if the monitored target requires authentication. The default value is **none**.

See Also

create, *delete*, *edit*, glob, *list*, *modify*, regex, *show*, *tmsh*

postgresql

Configures a PostgreSQL® monitor.

Syntax

Configure the **postgresql** component within the **ltm monitor** module using the syntax in the following sections.

Create/Modify

```
create postgresql [name]
modify postgresql [name]
    app-service [[string] | none]
    count [integer]
    database [ [name] | none]
    debug [no | yes]
    defaults-from [name]
    description [string]
    destination [ip address][port]
    interval [integer]
    manual-resume [enabled | disabled]
    password [none | [password] ]
    recv [none | [string] ]
    recv-column [none | [string] ]
    recv-row [none | [string] ]
    send [none | [string] ]
    time-until-up [integer]
    timeout [integer]
    up-interval [integer]
    username [[name] | none]
edit postgresql [ [ [name] | [glob] | [regex] ] ... ]
    all-properties
    non-default-properties
```

Display

```
list postgresql
list postgresql [ [ [name] | [glob] | [regex] ] ... ]
show postgresql [ [ [name] | [glob] | [regex] ] ... ]
show running-config postgresql
show running-config postgresql [ [ [name] | [glob] | [regex] ] ... ]
    all-properties
    non-default-properties
    one-line
    partition
```

Delete

```
delete postgresql [name]
```

◆ Note

You cannot delete default monitors.

Description

You can use the **postgresql** component to configure a custom monitor, or you can use the default PostgreSQL monitor that the Local Traffic Manager provides. This type of monitor verifies PostgreSQL-based services.

Examples

create postgresql my_postgresql defaults-from postgresql

Creates a monitor named **my_postgresql** that inherits properties from the default PostgreSQL monitor.

list postgresql

Displays the properties of all of the PostgreSQL monitors.

Options

- **app-service**
  Specifies the name of the application service to which the monitor belongs. The default value is **none**. **Note:** If the **strict-updates** option is **enabled** on the application service that owns the object, you cannot modify or delete the monitor. Only the application service can modify or delete the monitor.
- **count**
  Specifies the number of monitor probes after which the connection to the database will be terminated. Count value of zero indicates that the connection will never be terminated. The default value is **zero**.
- **database**
  Specifies the name of the database with which the monitor attempts to communicate. The default value is **none**.
- **debug**
  Specifies whether the monitor sends error messages and additional information to a log file created and labeled specifically for this monitor. You can use the log information to help diagnose and troubleshoot unsuccessful health checks. The default value is **no**.
  The options are:
  - **no**
    Specifies that the system does not redirect error messages and additional information related to this monitor.
  - **yes**
    Specifies that the system redirects error messages and additional information to the /var/log/monitors/<monitor_name>-<node_name>-<port>.log file.
- **defaults-from**
  Specifies the name of the monitor from which you want your custom monitor to inherit settings. The default value is **postgresql**.

- **description**
  User defined description.
- **destination**
  Specifies the IP address and service port of the resource that is the destination of this monitor. The default value is ***:***.
  Possible values are:
  - ***:***
    Specifies to perform a health check on the IP address and port supplied by a pool member.
  - ***:port**
    Specifies to perform a health check on the server with the IP address supplied by the pool member and the port you specify.
  - **IP address:port**
    Specifies to mark a pool member **up** or **down** based on the response of the server at the IP address and port you specify.
- **glob**
  Displays the items that match the **glob** expression. See **help glob** for a description of **glob** expression syntax.
- **interval**
  Specifies, in seconds, the frequency at which the system issues the monitor check when either the resource is **down** or the status of the resource is unknown. The default value is **30** seconds.

Important

*F5 Networks recommends that when you configure this option and the **up-interval** option, whichever value is greater be a multiple of the lesser value to allow for an even distribution of monitor checks among all monitors.*

- **manual-resume**
  Specifies whether the system automatically changes the status of a resource to **up** at the next successful monitor check. The default value of the manual-resume option is **disabled**.
  Note that if you set the **manual-resume** option to **enabled**, you must manually mark the resource as **up** before the system can use it for load balancing connections.
- **name**
  Specifies a unique name for the component. This option is required for the commands **create**, **delete**, and **modify**.
- **partition**
  Displays the administrative partition within which the component resides.
- **password**
  Specifies the password if the monitored target requires authentication. The default value is **none**.

- **recv**
  Specifies the text string that the monitor looks for in the returned resource. The default value is **none**.
  The most common receive expressions contain a text string that is included in a field in your database. If you do not specify a value for both the **send** and **recv** options, the monitor performs a simple service check and connect only.
- **recv-column**
  Specifies the column in the database where the system expects the specified Receive String to be located. Specify this option only if you configure the **send** and **recv** options. The default value is **none**.
- **recv-row**
  Specifies the row in the database where the system expects the specified Receive String to be located. Specify this option only if you configure the **send** and **recv** options. The default value is **none**.
- **regex**
  Displays the items that match the regular expression. The regular expression must be preceded by an at sign (@[regular expression]) to indicate that the identifier is a regular expression. See **help regex** for a description of regular expression syntax.
- **send**
  Specifies the SQL query that the monitor sends to the target database, for example, **SELECT count(*) FROM mytable**.
  If this value is null, then a valid connection suffices to determine that the service is **up**. In this case, the system does not need the recv option and ignores the option even if not null.
- **time-until-up**
  Specifies the amount of time, in seconds, after the first successful response before a node is marked **up**. A value of **0** (zero) causes a node to be marked **up** immediately after a valid response is received from the node. The default value is **0** (zero).
- **timeout**
  Specifies the number of seconds the target has in which to respond to the monitor request. The default value is **91** seconds.
  If the target responds within the set time period, it is considered **up**. If the target does not respond within the set time period, it is considered **down**. Also, if the target responds with a RESET packet, the system immediately flags the target as **down** without waiting for the timeout interval to expire.

- **up-interval**
  Specifies, in seconds, the frequency at which the system issues the monitor check when the resource is **up**. The default value is **0** (zero), which specifies that the system uses the value of the **interval** option whether the resource is **up** or **down**.

Important

*F5 Networks recommends that when you configure this option and the **interval** option, whichever value is greater be a multiple of the lesser value to allow for an even distribution of monitor checks among all monitors.*

- **username**
  Specifies the username, if the monitored target requires authentication. The default value is **none**.

See Also

create, *delete*, *edit*, glob, *list*, *modify*, regex, *show*, *tmsh*

radius

Configures a Remote Access Dial-in User Service (RADIUS) monitor.

Syntax

Configure the **radius** component within the **ltm monitor** module using the syntax in the following sections.

Create/Modify

```
create radius [name]
modify radius [name]
    app-service [[string] | none]
    debug [no | yes]
    defaults-from [name]
    description [string]
    destination [ip address][port]
    interval [integer]
    manual-resume [enabled | disabled]
    nas-ip-address [ [ip address] | none]
    password [none | [password] ]
    secret [none | [secret] ]
    time-until-up [integer]
    timeout [integer]
    up-interval [integer]
    username [ [name] | none]
edit radius [ [ [name] | [glob] | [regex] ] ... ]
    all-properties
    non-default-properties
```

Display

```
list radius
list radius [ [ [name] | [glob] | [regex] ] ... ]
show radius [ [ [name] | [glob] | [regex] ] ... ]
show running-config radius
show running-config radius [ [ [name] | [glob] | [regex] ] ... ]
    all-properties
    non-default-properties
    one-line
    partition
```

Delete

```
delete radius [name]
```

◆ Note

You cannot delete default monitors.

Description

You can use the **radius** component to configure a custom monitor, or you can use the default RADIUS monitor that the Local Traffic Manager provides. This type of monitor verifies the RADIUS service by attempting to authenticate the specified user.

Examples

create radius my_radius defaults-from radius

Creates a monitor named **my_radius** that inherits properties from the default RADIUS monitor.

list radius

Displays the properties of all of the RADIUS monitors.

Options

- **app-service**
  Specifies the name of the application service to which the monitor belongs. The default value is **none**. **Note:** If the **strict-updates** option is **enabled** on the application service that owns the object, you cannot modify or delete the monitor. Only the application service can modify or delete the monitor.
- **debug**
  Specifies whether the monitor sends error messages and additional information to a log file created and labeled specifically for this monitor. You can use the log information to help diagnose and troubleshoot unsuccessful health checks. The default value is **no**.
  The options are:
  - **no**
    Specifies that the system does not redirect error messages and additional information related to this monitor.
  - **yes**
    Specifies that the system redirects error messages and additional information to the /var/log/monitors/<monitor_name>-<node_name>-<port>.log file.
- **defaults-from**
  Specifies the name of the monitor from which you want your custom monitor to inherit settings. The default value is **radius**.
- **description**
  User defined description.
- **destination**
  Specifies the IP address and service port of the resource that is the destination of this monitor. The default value is ***:***.
  Possible values are:

- ***:***
  Specifies to perform a health check on the IP address and port supplied by a pool member.
- ***:port**
  Specifies to perform a health check on the server with the IP address supplied by the pool member and the port you specify.
- **IP address:port**
  Specifies to mark a pool member **up** or **down** based on the response of the server at the IP address and port you specify.

◆ **glob**
Displays the items that match the **glob** expression. See **help glob** for a description of **glob** expression syntax.

◆ **interval**
Specifies, in seconds, the frequency at which the system issues the monitor check when either the resource is **down** or the status of the resource is unknown. The default value is **10** seconds.

Important

*F5 Networks recommends that when you configure this option and the **up-interval** option, whichever value is greater be a multiple of the lesser value to allow for an even distribution of monitor checks among all monitors.*

◆ **manual-resume**
Specifies whether the system automatically changes the status of a resource to **up** at the next successful monitor check. The default value of the manual-resume option is **disabled**.
Note that if you set the **manual-resume** option to **enabled**, you must manually mark the resource as **up** before the system can use it for load balancing connections.

◆ **name**
Specifies a unique name for the component. This option is required for the commands **create**, **delete**, and **modify**.

◆ **nas-ip-address**
Specifies the network access server IP address that the system uses to identify itself to the RADIUS server. With this option, multiple BIG-IP systems can appear as a single network access device to the RADIUS server. The default value is **none**.

◆ **partition**
Displays the administrative partition within which the component resides.

◆ **password**
Specifies the password if the monitored target requires authentication. The default value is **none**.

- **regex**
  Displays the items that match the regular expression. The regular expression must be preceded by an at sign (@[regular expression]) to indicate that the identifier is a regular expression. See **help regex** for a description of regular expression syntax.
- **secret**
  Specifies the secret the monitor must use when contacting the resource. The default value is **none**.
- **time-until-up**
  Specifies the amount of time, in seconds, after the first successful response before a node is marked **up**. A value of **0** (zero) causes a node to be marked **up** immediately after a valid response is received from the node. The default value is **0** (zero).
- **timeout**
  Specifies the number of seconds the target has in which to respond to the monitor request. The default value is **31** seconds.
  If the target responds within the set time period, it is considered **up**. If the target does not respond within the set time period, it is considered **down**. Also, if the target responds with a RESET packet, the system immediately flags the target as **down** without waiting for the timeout interval to expire.
- **up-interval**
  Specifies, in seconds, the frequency at which the system issues the monitor check when the resource is **up**. The default value is **0** (zero), which specifies that the system uses the value of the **interval** option whether the resource is **up** or **down**.

Important

*F5 Networks recommends that when you configure this option and the **interval** option, whichever value is greater be a multiple of the lesser value to allow for an even distribution of monitor checks among all monitors.*

- **username**
  Specifies the username, if the monitored target requires authentication. The default value is **none**.

See Also

create, *delete*, *edit*, glob, *list*, *modify*, regex, *show*, *tmsh*

radius-accounting

Configures a RADIUS accounting monitor for the BIG-IP® Local Traffic Manager.

Syntax

Configure the **radius-accounting** component within the **ltm monitor** module using the syntax shown in the following sections.

Create/Modify

```
create radius-accounting [name]
modify radius-accounting [name]
    app-service [[string] | none]
    debug [no | yes]
    defaults-from [ [name] | none]
    description [string]
    destination [ip address]
    interval [integer]
    manual-resume [disabled | enabled]
    nas-ip-address [ip address]
    secret [string]
    time-until-up [integer]
    timeout [integer]
    up-interval [integer]
    username [none | [string] ]
edit radius-accounting [ [ [name] | [glob] | [regex] ] ...]
     all-properties
     non-default-properties
```

Display

```
list radius-accounting
list radius-accounting [ [ [name] | [glob] | [regex] ] ...]
show radius-accounting [ [ [name] | [glob] | [regex] ] ...]
show running-config radius-accounting
show running-config radius-accounting [ [ [name] | [glob] |
                                          [regex] ] ...]
    all-properties
    non-default-properties
    one-line
    partition
```

Delete

```
delete radius-accounting [name]
```

◆ Note

You cannot delete default monitors.

Description

You can use the **radius-accounting** component to configure a custom monitor, or you can use the default RADIUS accounting monitor that the Local Traffic Manager provides. This type of monitor provides information about the usage of the RADIUS service for accounting purposes.

Examples

create radius-accounting my_radius_acct defaults-from radius_accounting

Creates a monitor named **my_radius_acct** that inherits properties from the default RADIUS accounting monitor.

list radius-accounting

Displays the properties of all of the RADIUS accounting monitors.

Options

- **app-service**
  Specifies the name of the application service to which the monitor belongs. The default value is **none**. **Note:** If the **strict-updates** option is **enabled** on the application service that owns the object, you cannot modify or delete the monitor. Only the application service can modify or delete the monitor.
- **debug**
  Specifies whether the monitor sends error messages and additional information to a log file created and labeled specifically for this monitor. You can use the log information to help diagnose and troubleshoot unsuccessful health checks. The default value is **no**.
  The options are:
  - **no**
    Specifies that the system does not redirect error messages and additional information related to this monitor.
  - **yes**
    Specifies that the system redirects error messages and additional information to the /var/log/monitors/<monitor_name>-<node_name>-<port>.log file.
- **defaults-from**
  Specifies the name of the monitor from which you want your custom monitor to inherit settings. The default value is **radius**.
- **description**
  User defined description.
- **destination**
  Specifies the IP address and service port of the resource that is the destination of this monitor. The default value is ***:***.
  Possible values are:

- ***:***
  Specifies to perform a health check on the IP address and port supplied by a pool member.
- ***:port**
  Specifies to perform a health check on the server with the IP address supplied by the pool member and the port you specify.
- **IP address:port**
  Specifies to mark a pool member **up** or **down** based on the response of the server at the IP address and port you specify.

◆ **glob**
Displays the items that match the **glob** expression. See **help glob** for a description of **glob** expression syntax.

◆ **interval**
Specifies, in seconds, the frequency at which the system issues the monitor check when either the resource is **down** or the status of the resource is unknown. The default value is **10** seconds.

Important

*F5 Networks recommends that when you configure this option and the **up-interval** option, whichever value is greater be a multiple of the lesser value to allow for an even distribution of monitor checks among all monitors.*

◆ **manual-resume**
Specifies whether the system automatically changes the status of a resource to **up** at the next successful monitor check. The default value of the **manual-resume** option is **disabled**.
Note that if you set the **manual-resume** option to **enabled**, you must manually mark the resource as **up** before the system can use it for load balancing connections.

◆ **name**
Specifies a unique name for the component. This option is required for the commands **create**, **delete**, and **modify**.

◆ **nas-ip-address**
Specifies the network access server IP address that the system uses to identify itself to the RADIUS server. Using this option, multiple BIG-IP® systems can appear as a single network access device to the RADIUS server. The default value is **none**.

◆ **partition**
Displays the administrative partition within which the component resides.

◆ **regex**
Displays the items that match the regular expression. The regular expression must be preceded by an at sign (@[regular expression]) to indicate that the identifier is a regular expression. See **help regex** for a description of regular expression syntax.

- **secret**
  Specifies the secret the monitor needs to communicate with the resource. The default value is **none**.
- **time-until-up**
  Specifies the amount of time in seconds after the first successful response before a node is marked up. A value of **0** (zero) causes a node to be marked up immediately after a valid response is received from the node. The default value is **0** (zero).
- **timeout**
  Specifies the number of seconds the target has in which to respond to the monitor request. The default value is **31** seconds.
  If the target responds within the set time period, it is considered **up**. If the target does not respond within the set time period, it is considered **down**. Also, if the target responds with a RESET packet, the system immediately flags the target as **down** without waiting for the timeout interval to expire.
- **up-interval**
  Specifies, in seconds, the frequency at which the system issues the monitor check when the resource is **up**. The default value is **0** (zero), which specifies that the system uses the value of the **interval** option whether the resource is **up** or **down**.

Important

*F5 Networks recommends that when you configure this option and the **interval** option, whichever value is greater be a multiple of the lesser value to allow for an even distribution of monitor checks among all monitors.*

- **username**
  Specifies the username, if the monitored target requires authentication. The default value is **none**.

See Also

create, *delete*, *edit*, glob, *pool*, *list*, *modify*, regex, *show*, *tmsh*

real-server

Configures a RealServer® monitor.

Syntax

Configure the **real-server** component within the **ltm monitor** module using the syntax in the following sections.

Create/Modify

```
create real-server [name]
modify real-server [name]
    app-service [[string] | none]
    defaults-from [name]
    description [string]
    interval [integer]
    metrics [ [metrics] | none]
    time-until-up [integer]
    timeout [integer]
edit real-server [ [ [name] | [glob] | [regex] ] ... ]
      all-properties
     non-default-properties
```

Display

```
list real-server
list real-server [ [ [name] | [glob] | [regex] ] ... ]
show real-server [ [ [name] | [glob] | [regex] ] ... ]
show running-config real-server
show running-config real-server [ [ [name] | [glob] | [regex] ] ... ]
    agent
    all-properties
    command
    method
    non-default-properties
    one-line
    partition
```

Delete

```
delete real-server [name]
```

◆ Note

You cannot delete default monitors.

Description

You can use the **real-server** component to configure a custom monitor, or you can use the default RealServer monitor that the Local Traffic Manager provides. This type of monitor checks the performance of a pool, pool member, or virtual server that is running the RealServer data collection agent, and then dynamically load balances traffic accordingly.

Examples

create real-server my_real-server defaults-from real_server

Creates a monitor named **my_real-server** that inherits properties from the default RealServer monitor.

list real-server

Displays the properties of all of the RealServer monitors.

Options

- **agent**
  Displays the agent for the monitor. The default agent is **Mozilla/4.0 (compatible: MSIE 5.0; Windows NT)**. You cannot modify the agent.
- **app-service**
  Specifies the name of the application service to which the monitor belongs. The default value is **none**. **Note:** If the **strict-updates** option is **enabled** on the application service that owns the object, you cannot modify or delete the monitor. Only the application service can modify or delete the monitor.
- **command**
  Displays the command that the system uses to obtain the metrics from the resource. See the documentation for this resource for information on available commands. You cannot modify the command.
- **defaults-from**
  Specifies the name of the monitor from which you want your custom monitor to inherit settings. The default value is **real-server**.
- **description**
  User defined description.
- **glob**
  Displays the items that match the **glob** expression. See **help glob** for a description of **glob** expression syntax.
- **interval**
  Specifies the frequency at which the system issues the monitor check. The default value is **5** seconds.
- **name**
  Specifies a unique name for the component. This option is required for the commands **create**, **delete**, and **modify**.

- **method**
  Displays the GET method. You cannot modify the method.
- **metrics**
  Specifies the performance metrics that the commands collect from the target. The default value is **ServerBandwidth:1.5, CPUPercentUsage, MemoryUsage, TotalClientCount**.
- **partition**
  Displays the administrative partition within which the component resides.
- **regex**
  Displays the items that match the regular expression. The regular expression must be preceded by an at sign (@[regular expression]) to indicate that the identifier is a regular expression. See **help regex** for a description of regular expression syntax.
- **time-until-up**
  Specifies the amount of time, in seconds, after the first successful response before a node is marked **up**. A value of **0** (zero) causes a node to be marked **up** immediately after a valid response is received from the node. The default value is **0** (zero).
- **timeout**
  Specifies the number of seconds the target has in which to respond to the monitor request. The default value is **16** seconds.
  If the target responds within the set time period, it is considered **up**. If the target does not respond within the set time period, it is considered **down**. Also, if the target responds with a RESET packet, the system immediately flags the target as **down** without waiting for the timeout interval to expire.

See Also

create, *delete*, *edit*, glob, *list*, *modify*, regex, *show*, *tmsh*

rpc

Configures a Remote Procedure Call (RPC) monitor.

Syntax

Configure the **rpc** component within the **ltm monitor** module using the syntax in the following sections.

Create/Modify

```
create rpc [name]
modify rpc [name]
    app-service [[string] | none]
    debug [no | yes]
    defaults-from [name]
    description [string]
    destination [ip address] [port]
    interval [integer]
    manual-resume [enabled | disabled]
    mode [tcp | udp]
    program-number [ [integer] | none]
    time-until-up [integer]
    timeout [integer]
    up-interval [integer]
    version-number [ [integer] | none]
edit rpc [ [ [name] | [glob] | [regex] ] ... ]
    all-properties
    non-default-properties
```

Display

```
list rpc
list rpc [ [ [name] | [glob] | [regex] ] ... ]
show rpc [ [ [name] | [glob] | [regex] ] ... ]
show running-config rpc
show running-config rpc [ [ [name] | [glob] | [regex] ] ... ]
    all-properties
    non-default-properties
    one-line
    partition
```

Delete

```
delete rpc [name]
```

◆ Note

You cannot delete default monitors.

Description

You can use the **rpc** component to configure a custom monitor, or you can use the default RPC monitor that the Local Traffic Manager provides. This type of monitor queries the RPC server, and verifies the availability of a given program.

Examples

create rpc my_rpc defaults-from rpc

Creates a monitor named **my_rpc** that inherits properties from the default RPC monitor.

list rpc

Displays the properties of all of the RPC monitors.

Options

- **app-service**
  Specifies the name of the application service to which the monitor belongs. The default value is **none**. **Note:** If the **strict-updates** option is **enabled** on the application service that owns the object, you cannot modify or delete the monitor. Only the application service can modify or delete the monitor.
- **debug**
  Specifies whether the monitor sends error messages and additional information to a log file created and labeled specifically for this monitor. You can use the log information to help diagnose and troubleshoot unsuccessful health checks.
  The default value is **no**. The options are:
  - **no**
    Specifies that the system does not redirect error messages and additional information related to this monitor.
  - **yes**
    Specifies that the system redirects error messages and additional information to the /var/log/monitors/<monitor_name>-<node_name>-<port>.log file.
- **defaults-from**
  Specifies the name of the monitor from which you want your custom monitor to inherit settings. The default value is **rpc**.
- **description**
  User defined description.
- **destination**
  Specifies the IP address and service port of the resource that is the destination of this monitor. The default value is ***:***.
  Possible values are:

- ***:***
  Specifies to perform a health check on the IP address and port supplied by a pool member.
- ***:port**
  Specifies to perform a health check on the server with the IP address supplied by the pool member and the port you specify.
- **IP address:port**
  Specifies to mark a pool member **up** or **down** based on the response of the server at the IP address and port you specify.

◆ **glob**
Displays the items that match the **glob** expression. See **help glob** for a description of **glob** expression syntax.

◆ **interval**
Specifies, in seconds, the frequency at which the system issues the monitor check when either the resource is **down** or the status of the resource is unknown. The default value is **10** seconds.

Important

*F5 Networks recommends that when you configure this option and the **up-interval** option, whichever value is greater be a multiple of the lesser value to allow for an even distribution of monitor checks among all monitors.*

◆ **manual-resume**
Specifies whether the system automatically changes the status of a resource to **up** at the next successful monitor check. The default value of the manual-resume option is **disabled**.
Note that if you set the **manual-resume** option to **enabled**, you must manually mark the resource as **up** before the system can use it for load balancing connections.

◆ **mode**
Specifies the protocol that the monitor uses to communicate with the target. The default value is tcp.
The options are:

- **tcp**
  Specifies that the monitor uses the TCP protocol to communicate with the target object.
- **udp**
  Specifies that the monitor uses the UDP protocol to communicate with the target object.

◆ **name**
Specifies a unique name for the component. This option is required for the commands **create**, **delete**, and **modify**.

◆ **partition**
Displays the administrative partition within which the component resides.

- **program-number**
  Specifies the number of the program for which you want the monitor to verify availability. The default value is **none**.
- **regex**
  Displays the items that match the regular expression. The regular expression must be preceded by an at sign (@[regular expression]) to indicate that the identifier is a regular expression. See **help regex** for a description of regular expression syntax.
- **time-until-up**
  Specifies the amount of time, in seconds, after the first successful response before a node is marked **up**. A value of **0** (zero) causes a node to be marked **up** immediately after a valid response is received from the node. The default value is **0** (zero).
- **timeout**
  Specifies the number of seconds the target has in which to respond to the monitor request. The default value is **31** seconds.
  If the target responds within the set time period, it is considered **up**. If the target does not respond within the set time period, it is considered **down**. Also, if the target responds with a RESET packet, the system immediately flags the target as **down** without waiting for the timeout interval to expire.
- **up-interval**
  Specifies, in seconds, the frequency at which the system issues the monitor check when the resource is **up**. The default value is **0** (zero), which specifies that the system uses the value of the **interval** option whether the resource is **up** or **down**.

Important

*F5 Networks recommends that when you configure this option and the **interval** option, whichever value is greater be a multiple of the lesser value to allow for an even distribution of monitor checks among all monitors.*

- **version-number**
  Specifies the number of the version for which you want the monitor to verify availability. The default value is **none**.

See Also

create, *delete*, *edit*, glob, *list*, *modify*, regex, *show*, *tmsh*

sasp

Configures a Server Application State Protocol (SASP) monitor.

Syntax

Configure the **sasp** component within the **ltm monitor** module using the syntax in the following sections.

Create/Modify

```
create sasp [name]
modify sasp [name]
    app-service [[string] | none]
    defaults-from [name]
    description [string]
    interval [integer]
    mode [pull | push]
    primary-address [ip address]
    protocol [tcp | udp]
    secondary-address [ [ip address] | none]
    service [none | [port] ]
    time-until-up [integer]
    timeout [integer]
edit sasp [ [ [name] | [glob] | [regex] ] ... ]
    all-properties
    non-default-properties
```

Display

```
list sasp
list sasp [ [ [name] | [glob] | [regex] ] ... ]
show sasp [ [ [name] | [glob] | [regex] ] ... ]
show running-config sasp
show running-config sasp [ [ [name] | [glob] | [regex] ] ... ]
    all-properties
    non-default-properties
    one-line
    partition
```

Delete

```
delete sasp [name]
```

◆ Note

You cannot delete default monitors.

Description

You can use the **sasp** component to configure a custom monitor, or you can use the default FTP monitor that the Local Traffic Manager provides. This type of monitor verifies the availability of IBM Group Workload Managers network resources.

Examples

create sasp my_sasp defaults-from sasp

Creates a monitor named **my_sasp** that inherits properties from the default SASP monitor.

list sasp

Displays the properties of all of the SASP monitors.

Options

- **app-service**
  Specifies the name of the application service to which the monitor belongs. The default value is **none**. **Note:** If the **strict-updates** option is **enabled** on the application service that owns the object, you cannot modify or delete the monitor. Only the application service can modify or delete the monitor.
- **defaults-from**
  Specifies the name of the monitor from which you want your custom monitor to inherit settings. The default value is **sasp**.
- **description**
  User defined description.
- **glob**
  Displays the items that match the **glob** expression. See **help glob** for a description of **glob** expression syntax.
- **interval**
  Specifies the frequency at which the system issues the monitor check. The default value is **auto**.
- **mode**
  Specifies whether the load balancer should send Get Weight Request messages (pull) or receive Send Weights messages (push) from the GWM. The default mode is pull.
- **name**
  Specifies a unique name for the component. This option is required for the commands **create**, **delete**, and **modify**.
- **partition**
  Displays the administrative partition within which the component resides.

- **primary-address**
  Specifies the IP address of the primary Group Workload Manager.
- **protocol**
  Specifies the protocol that the monitor uses to communicate with the target. The default value is **tcp**.
- **regex**
  Displays the items that match the regular expression. The regular expression must be preceded by an at sign (@[regular expression]) to indicate that the identifier is a regular expression. See **help regex** for a description of regular expression syntax.
- **secondary-address**
  Specifies the IP address of the secondary Group Workload Manager.
- **service**
  Specifies the port through which the SASP monitor communicates with the Group Workload Manager. The default port is **3860**.
- **time-until-up**
  Specifies the amount of time, in seconds, after the first successful response before a node is marked **up**. A value of **0** (zero) causes a node to be marked **up** immediately after a valid response is received from the node. The default value is **0** (zero).
- **timeout**
  Specifies the number of seconds the target has in which to respond to the monitor request. The default value is **100** seconds.
  If the target responds within the set time period, it is considered **up**. If the target does not respond within the set time period, it is considered **down**. Also, if the target responds with a RESET packet, the system immediately flags the target as **down** without waiting for the timeout interval to expire.

See Also

create, *delete*, *edit*, glob, *list*, *modify*, regex, *show*, *tmsh*

scripted

Configures a Scripted monitor.

Syntax

Configure the **scripted** component within the **ltm monitor** module using the syntax in the following sections.

Create/Modify

```
create scripted [name]
modify scripted [name]
    app-service [[string] | none]
    debug [no | yes]
    defaults-from [name]
    description [string]
    destination [ip address] [port]
    filename [ [filename] | none]
    interval [integer]
    manual-resume [enabled | disabled]
    time-until-up [integer]
    timeout [integer]
    up-interval [integer]
edit scripted [ [ [name] | [glob] | [regex] ] ... ]
    all-properties
    non-default-properties
```

Display

```
list scripted
list scripted [ [ [name] | [glob] | [regex] ] ... ]
show scripted [ [ [name] | [glob] | [regex] ] ... ]
show running-config scripted
show running-config scripted [ [ [name] | [glob] | [regex] ] ... ]
    all-properties
    non-default-properties
    one-line
    partition
```

Delete

```
delete scripted [name]
```

◆ Note

You cannot delete default monitors.

Description

You can use the **scripted** component to configure a custom monitor, or you can use the default scripted monitor that the Local Traffic Manager provides.

Examples

create scripted my_scripted defaults-from scripted

Creates a monitor named **my_scripted** that inherits properties from the default scripted monitor.

list scripted

Displays the properties of all of the scripted monitors.

Options

- **app-service**
  Specifies the name of the application service to which the monitor belongs. The default value is **none**. **Note:** If the **strict-updates** option is **enabled** on the application service that owns the object, you cannot modify or delete the monitor. Only the application service can modify or delete the monitor.
- **debug**
  Specifies whether the monitor sends error messages and additional information to a log file created and labeled specifically for this monitor. You can use the log information to help diagnose and troubleshoot unsuccessful health checks.
  The default value is **no**. The options are:
  - **no**
    Specifies that the system does not redirect error messages and additional information related to this monitor.
  - **yes**
    Specifies that the system redirects error messages and additional information to the /var/log/monitors/<monitor_name>-<node_name>-<port>.log file.
- **defaults-from**
  Specifies the name of the monitor from which you want your custom monitor to inherit settings. The default value is **scripted**.
- **description**
  User defined description.
- **destination**
  Specifies the IP address and service port of the resource that is the destination of this monitor. The default value is ***:***.
  Possible values are:

- ***:***
  Specifies to perform a health check on the IP address and port supplied by a pool member.
- ***:port**
  Specifies to perform a health check on the server with the IP address supplied by the pool member and the port you specify.
- **IP address:port**
  Specifies to mark a pool member **up** or **down** based on the response of the server at the IP address and port you specify.

◆ **filename**
Specifies the name of a file in the **/config/eav/** directory on the system. The user-created file contains the send and expect data that the monitor uses for the monitor check. The default value is **none**.

◆ **glob**
Displays the items that match the **glob** expression. See **help glob** for a description of **glob** expression syntax.

◆ **interval**
Specifies, in seconds, the frequency at which the system issues the monitor check when either the resource is **down** or the status of the resource is unknown. The default value is **10** seconds.

Important

*F5 Networks recommends that when you configure this option and the **up-interval** option, whichever value is greater be a multiple of the lesser value to allow for an even distribution of monitor checks among all monitors.*

◆ **manual-resume**
Specifies whether the system automatically changes the status of a resource to **up** at the next successful monitor check. The default value of the manual-resume option is **disabled**.
Note that if you set the **manual-resume** option to **enabled**, you must manually mark the resource as **up** before the system can use it for load balancing connections.

◆ **name**
Specifies a unique name for the component. This option is required for the commands **create**, **delete**, and **modify**.

◆ **partition**
Displays the administrative partition within which the component resides.

◆ **regex**
Displays the items that match the regular expression. The regular expression must be preceded by an at sign (@[regular expression]) to indicate that the identifier is a regular expression. See **help regex** for a description of regular expression syntax.

- **time-until-up**
  Specifies the amount of time, in seconds, after the first successful response before a node is marked **up**. A value of **0** (zero) causes a node to be marked **up** immediately after a valid response is received from the node. The default value is **0** (zero).
- **timeout**
  Specifies the number of seconds the target has in which to respond to the monitor request. The default value is **31** seconds.
  If the target responds within the set time period, it is considered **up**. If the target does not respond within the set time period, it is considered **down**. Also, if the target responds with a RESET packet, the system immediately flags the target as **down** without waiting for the timeout interval to expire.
- **up-interval**
  Specifies, in seconds, the frequency at which the system issues the monitor check when the resource is **up**. The default value is **0** (zero), which specifies that the system uses the value of the **interval** option whether the resource is **up** or **down**.

Important

*F5 Networks recommends that when you configure this option and the **interval** option, whichever value is greater be a multiple of the lesser value to allow for an even distribution of monitor checks among all monitors.*

See Also

create, *delete*, *edit*, glob, *list*, *modify*, regex, *show*, *tmsh*

sip

Configures a Session Initiation Protocol (SIP) monitor.

Syntax

Configure the **sip** component within the **ltm monitor** module using the syntax in the following sections.

Create/Modify

```
create sip [name]
modify sip [name]
    app-service [[string] | none]
    cert [ [cert list] | none]
    cipherlist [string]
    compatibility [enabled | disabled]
    debug [ no | yes]
    defaults-from [name]
    description [string]
    destination [ip address][port]
    filter [any | none | status]
    filter-neg [any | none | status]
    headers [ [new line separated headers] | none]
    interval [integer]
    key [ [key] | none]
    manual-resume [enabled | disabled]
    mode [sips | tcp | tls | udp]
    request [none | [string] ]
    time-until-up [integer]
    up-interval [integer]
    username [ [name] | none]
edit sip [ [ [name] | [glob] | [regex] ] ... ]
    all-properties
    non-default-properties
```

Display

```
list sip
list sip [ [ [name] | [glob] | [regex] ] ... ]
show sip [ [ [name] | [glob] | [regex] ] ... ]
show running-config sip
show running-config sip [ [ [name] | [glob] | [regex] ] ... ]
    all-properties
    non-default-properties
    one-line
    partition
```

Delete

```
delete sip [name]
```

◆ Note

You cannot delete default monitors.

Description

You can use the **sip** component to configure a custom monitor, or you can use the default SIP monitor that the Local Traffic Manager provides. This type of monitor checks the status of SIP Call-ID services on a device. The SIP protocol enables real-time messaging, voice, data, and video.

Examples

create sip my_sip defaults-from sip

Creates a monitor named **my_sip** that inherits properties from the default SIP monitor.

list sip

Displays the properties of all of the SIP monitors.

Options

- **app-service**
  Specifies the name of the application service to which the monitor belongs. The default value is **none**. **Note:** If the **strict-updates** option is **enabled** on the application service that owns the object, you cannot modify or delete the monitor. Only the application service can modify or delete the monitor.
- **cert**
  Specifies a fully-qualified path for a client certificate that the monitor sends to the target SSL server. The default value is **none**.
- **cipherlist**
  Specifies the list of ciphers for this monitor. The default value is **DEFAULT:+SHA:+3DES:+kEDH**.
- **compatibility**
  Specifies, when enabled, that the SSL options setting (in OpenSSL) is set to ALL. The default value is **enabled**.
- **debug**
  Specifies whether the monitor sends error messages and additional information to a log file created and labeled specifically for this monitor. You can use the log information to help diagnose and troubleshoot unsuccessful health checks.
  The default value is **no**. The options are:
  - **no**
    Specifies that the system does not redirect error messages and additional information related to this monitor.
  - **yes**
    Specifies that the system redirects error messages and additional information to the /var/log/monitors/<monitor_name>-<node_name>-<port>.log file.

- **defaults-from**
  Specifies the name of the monitor from which you want your custom monitor to inherit settings. The default value is **sip**.
- **description**
  User defined description.
- **destination**
  Specifies the IP address and service port of the resource that is the destination of this monitor. The default value is ***:***.
  Possible values are:
  - ***:***
    Specifies to perform a health check on the IP address and port supplied by a pool member.
  - ***:port**
    Specifies to perform a health check on the server with the IP address supplied by the pool member and the port you specify.
  - **IP address:port**
    Specifies to mark a pool member **up** or **down** based on the response of the server at the IP address and port you specify.
- **filter**
  Specifies the SIP status codes that the target can return to be considered **up**. By default the system always accepts status codes whose value is in the 100, 200 or 300s.
  The options are:
  - **any**
    Specifies that the monitor accepts any SIP status codes.
  - **none**
    Specifies that the monitor does not accept any other SIP status codes. This is the default value.
  - **status**
    Specifies one or more status codes that you want to add to the monitor.
- **filter-neg**
  Specifies the SIP status codes that the target can return to be considered **down**. By default the system always accepts status codes according to **sip-monitor.filter**. After checking that, the status code is checked against this key. If a code is also in **sip-monitor.filter**, the node is marked **up**.
  The options are:
  - **any**
    Specifies that the monitor rejects all SIP status codes that are not in **sip-monitor.filter**.
  - **none**
    Specifies that the monitor does not specifically reject any other SIP status codes. This is the default value.
  - **status**
    Specifies one or more status codes that you want to add to the monitor.

- **glob**
  Displays the items that match the **glob** expression. See **help glob** for a description of **glob** expression syntax.
- **headers**
  Specifies the set of SIP headers in the SIP message that is sent to the target. Separate each header with a new line. The default value is **none**.
- **interval**
  Specifies, in seconds, the frequency at which the system issues the monitor check when either the resource is **down** or the status of the resource is unknown. The default value is **5** seconds.

Important

*F5 Networks recommends that when you configure this option and the **up-interval** option, whichever value is greater be a multiple of the lesser value to allow for an even distribution of monitor checks among all monitors.*

- **key**
  Specifies the key if the monitored target requires authentication. The default value is **none**.
- **manual-resume**
  Specifies whether the system automatically changes the status of a resource to **up** at the next successful monitor check. The default value of the manual-resume option is **disabled**.
  Note that if you set the **manual-resume** option to **enabled**, you must manually mark the resource as **up** before the system can use it for load balancing connections.
- **mode**
  Specifies the protocol that the monitor uses to communicate with the target. The default mode is udp. The options are:
  - **sips**
    Specifies that the monitor uses SIPS to communicate with the target.
  - **tcp**
    Specifies that the monitor uses TCP to communicate with the target.
  - **tls**
    Specifies that the monitor uses TLS to communicate with the target, and the SIP URI is SIPS.
  - **udp**
    Specifies that the monitor uses UDP to communicate with the target.
- **name**
  Specifies a unique name for the component. This option is required for the commands **create**, **delete**, and **modify**.
- **partition**
  Displays the administrative partition within which the component resides.

- **regex**
  Displays the items that match the regular expression. The regular expression must be preceded by an at sign (@[regular expression]) to indicate that the identifier is a regular expression. See **help regex** for a description of regular expression syntax.
- **request**
  Specifies the SIP request line in the SIP message that is sent to the target. The default value is **none**.
- **time-until-up**
  Specifies the amount of time, in seconds, after the first successful response before a node is marked **up**. A value of **0** (zero) causes a node to be marked **up** immediately after a valid response is
- **timeout**
  Specifies the number of seconds the target has in which to respond to the monitor request. The default value is **16** seconds.
  If the target responds within the set time period, it is considered **up**. If the target does not respond within the set time period, it is considered **down**. Also, if the target responds with a RESET packet, the system immediately flags the target as **down** without waiting for the timeout interval to expire.
- **up-interval**
  Specifies, in seconds, the frequency at which the system issues the monitor check when the resource is **up**. The default value is **0** (zero), which specifies that the system uses the value of the **interval** option whether the resource is **up** or **down**.

Important

*F5 Networks recommends that when you configure this option and the **interval** option, whichever value is greater be a multiple of the lesser value to allow for an even distribution of monitor checks among all monitors.*

See Also

create, *delete*, *edit*, glob, *list*, *modify*, regex, *show*, *tmsh*

smb

Configures a Server Message Bloc (SMB)/Common Internet File System (CIFS) monitor.

Syntax

Configure the **smb** component within the **ltm monitor** module using the syntax in the following sections.

Create/Modify

```
create smb [name]
modify smb [name]
    app-service [[string] | none]
    debug [no | yes]
    defaults-from [name]
    description [string]
    destination [ip address][port]
    get [none | [filename] ]
    interval [integer]
    manual-resume [enabled | disabled]
    password [none | [password] ]
    server [ [NETBIOS name] | none]
    service [ [[name] | [integer]] | none]
    time-until-up [integer]
    timeout [integer]
    up-interval [integer]
    username [ [name] | none]
edit smb [ [ [name] | [glob] | [regex] ] ... ]
    all-properties
    non-default-properties
```

Display

```
list smb
list smb [ [ [name] | [glob] | [regex] ] ... ]
show smb [ [ [name] | [glob] | [regex] ] ... ]
show running-config smb
show running-config smb [ [ [name] | [glob] | [regex] ] ... ]
    all-properties
    non-default-properties
    one-line
    partition
```

Delete

```
delete smb [name]
```

◆ Note

You cannot delete default monitors.

Description

You can use the **smb** component to configure a custom monitor, or you can use the default SMB monitor that the Local Traffic Manager provides. This type of monitor verifies the availability of an SMB/CIFS server. You can use this type of monitor to either check the availability of the server as a whole, the availability of a specific service on the server, or the availability of a specific file used by a service.

Examples

create smb my_smb defaults-from smb

Creates a monitor named **my_smb** that inherits properties from the default SMB monitor.

list smb

Displays the properties of all of the SMB monitors.

Options

- **app-service**
  Specifies the name of the application service to which the monitor belongs. The default value is **none**. **Note:** If the **strict-updates** option is **enabled** on the application service that owns the object, you cannot modify or delete the monitor. Only the application service can modify or delete the monitor.
- **debug**
  Specifies whether the monitor sends error messages and additional information to a log file created and labeled specifically for this monitor. You can use the log information to help diagnose and troubleshoot unsuccessful health checks. The default value is **no**.
  The options are:
  - **no**
    Specifies that the system does not redirect error messages and additional information related to this monitor.
  - **yes**
    Specifies that the system redirects error messages and additional information to the /var/log/monitors/<monitor_name>-<node_name>-<port>.log file.
- **defaults-from**
  Specifies the name of the monitor from which you want your custom monitor to inherit settings. The default value is **smb**.
- **description**
  User defined description.

- **destination**
  Specifies the IP address and service port of the resource that is the destination of this monitor. The default value is ***:***.
  Possible values are:
  - ***:***
    Specifies to perform a health check on the IP address and port supplied by a pool member.
  - ***:port**
    Specifies to perform a health check on the server with the IP address supplied by the pool member and the port you specify.
  - **IP address:port**
    Specifies to mark a pool member **up** or **down** based on the response of the server at the IP address and port you specify.
- **get**
  Specifies a file associated with a service. The default value is **none**.
  The monitor uses the relative path to the service itself when attempting to locate the file. You are not required to specify a value for this option; however, if you elect to use this option you must also specify a value for the **service** option.
- **glob**
  Displays the items that match the **glob** expression. See **help glob** for a description of **glob** expression syntax.
- **interval**
  Specifies, in seconds, the frequency at which the system issues the monitor check when either the resource is **down** or the status of the resource is unknown. The default value is **10** seconds.

Important

*F5 Networks recommends that when you configure this option and the **up-interval** option, whichever value is greater be a multiple of the lesser value to allow for an even distribution of monitor checks among all monitors.*

- **manual-resume**
  Specifies whether the system automatically changes the status of a resource to **up** at the next successful monitor check. The default value of the manual-resume option is **disabled**.
  Note that if you set the **manual-resume** option to **enabled**, you must manually mark the resource as **up** before the system can use it for load balancing connections.
- **name**
  Specifies a unique name for the component. This option is required for the commands **create**, **delete**, and **modify**.
- **partition**
  Displays the administrative partition within which the component resides.

- **password**
  Specifies the password if the monitored target requires authentication. The default value is **none**.
- **regex**
  Displays the items that match the regular expression. The regular expression must be preceded by an at sign (@[regular expression]) to indicate that the identifier is a regular expression. See **help regex** for a description of regular expression syntax.
- **server**
  Specifies the NetBIOS name of the SMB/CIFS server for which this monitor checks for availability. You must specify a server for this monitor to function. The default value is **none**.
- **service**
  Specifies a specific service on the SMB/CIFS for which you want to verify availability. The default value is **none**.
- **time-until-up**
  Specifies the amount of time, in seconds, after the first successful response before a node is marked **up**. A value of **0** (zero) causes a node to be marked **up** immediately after a valid response is received from the node. The default value is **0** (zero).
- **timeout**
  Specifies the number of seconds the target has in which to respond to the monitor request. The default value is **31** seconds.
  If the target responds within the set time period, it is considered **up**. If the target does not respond within the set time period, it is considered **down**. Also, if the target responds with a RESET packet, the system immediately flags the target as **down** without waiting for the timeout interval to expire.
- **up-interval**
  Specifies, in seconds, the frequency at which the system issues the monitor check when the resource is **up**. The default value is **0** (zero), which specifies that the system uses the value of the **interval** option whether the resource is **up** or **down**.

Important

*F5 Networks recommends that when you configure this option and the **interval** option, whichever value is greater be a multiple of the lesser value to allow for an even distribution of monitor checks among all monitors.*

- **username**
  Specifies the user name if the monitored target requires authentication. The default value is **none**.

See Also

create, *delete*, *edit*, glob, *list*, *modify*, regex, *show*, *tmsh*

smtp

Configures a Simple Mail Transport Protocol (SMTP) monitor.

Syntax

Configure the **smtp** component within the **ltm monitor** module using the syntax in the following sections.

Create/Modify

```
create smtp [name]
modify smtp [name]
    app-service [[string] | none]
    debug [no | yes]
    defaults-from [name]
    description [string]
    destination [ip address][port]
    domain [ [name] | none]
    interval [integer]
    manual-resume [enabled | disabled]
    time-until-up [integer]
    timeout [integer]
    up-interval [integer]
edit smtp [ [ [name] | [glob] | [regex] ] ... ]
    all-properties
    non-default-properties
```

Display

```
list smtp
list smtp [ [ [name] | [glob] | [regex] ] ... ]
show smtp [ [ [name] | [glob] | [regex] ] ... ]
show running-config smtp
show running-config smtp [ [ [name] | [glob] | [regex] ] ... ]
    all-properties
    non-default-properties
    one-line
    partition
```

Delete

```
delete smtp [name]
```

◆ Note

You cannot delete default monitors.

Description

You can use the **smtp** component to configure a custom monitor, or you can use the default SMTP monitor that the Local Traffic Manager provides. This type of monitor checks the status of a pool, pool member, or virtual server by issuing standard SMTP commands.

Examples

create smtp my_smtp defaults-from smtp

Creates a monitor named **my_smtp** that inherits properties from the default SMTP monitor.

list smtp

Displays the properties of all of the SMTP monitors.

Options

- **app-service**
  Specifies the name of the application service to which the monitor belongs. The default value is **none**. **Note:** If the **strict-updates** option is **enabled** on the application service that owns the object, you cannot modify or delete the monitor. Only the application service can modify or delete the monitor.
- **debug**
  Specifies whether the monitor sends error messages and additional information to a log file created and labeled specifically for this monitor. You can use the log information to help diagnose and troubleshoot unsuccessful health checks. The default value is **no**.
  The options are:
  - **no**
    Specifies that the system does not redirect error messages and additional information related to this monitor.
  - **yes**
    Specifies that the system redirects error messages and additional information to the /var/log/monitors/<monitor_name>-<node_name>-<port>.log file.
- **defaults-from**
  Specifies the name of the monitor from which you want your custom monitor to inherit settings. The default value is **smtp**.
- **description**
  User defined description.
- **destination**
  Specifies the IP address and service port of the resource that is the destination of this monitor. The default value is ***:***.
  Possible values are:

- ***:***
  Specifies to perform a health check on the IP address and port supplied by a pool member.
- ***:port**
  Specifies to perform a health check on the server with the IP address supplied by the pool member and the port you specify.
- **IP address:port**
  Specifies to mark a pool member **up** or **down** based on the response of the server at the IP address and port you specify.

◆ **domain**
Specifies the domain name to check, for example, **bigipinternal.com**. The default value is **none**.

◆ **glob**
Displays the items that match the **glob** expression. See **help glob** for a description of **glob** expression syntax.

◆ **interval**
Specifies, in seconds, the frequency at which the system issues the monitor check when either the resource is **down** or the status of the resource is unknown. The default value is **5** seconds.

Important

*F5 Networks recommends that when you configure this option and the **up-interval** option, whichever value is greater be a multiple of the lesser value to allow for an even distribution of monitor checks among all monitors.*

◆ **manual-resume**
Specifies whether the system automatically changes the status of a resource to **up** at the next successful monitor check. The default value of the manual-resume option is **disabled**.
Note that if you set the **manual-resume** option to **enabled**, you must manually mark the resource as **up** before the system can use it for load balancing connections.

◆ **name**
Specifies a unique name for the component. This option is required for the commands **create**, **delete**, and **modify**.

◆ **partition**
Displays the administrative partition within which the component resides.

◆ **regex**
Displays the items that match the regular expression. The regular expression must be preceded by an at sign (@[regular expression]) to indicate that the identifier is a regular expression. See **help regex** for a description of regular expression syntax.

- **time-until-up**
  Specifies the amount of time, in seconds, after the first successful response before a node is marked **up**. A value of **0** (zero) causes a node to be marked **up** immediately after a valid response is received from the node. The default value is **0** (zero).
- **timeout**
  Specifies the number of seconds the target has in which to respond to the monitor request. The default value is **16** seconds.
  If the target responds within the set time period, it is considered **up**. If the target does not respond within the set time period, it is considered **down**. Also, if the target responds with a RESET packet, the system immediately flags the target as **down** without waiting for the timeout interval to expire.
- **up-interval**
  Specifies, in seconds, the frequency at which the system issues the monitor check when the resource is **up**. The default value is **0** (zero), which specifies that the system uses the value of the **interval** option whether the resource is **up** or **down**.

Important

*F5 Networks recommends that when you configure this option and the **interval** option, whichever value is greater be a multiple of the lesser value to allow for an even distribution of monitor checks among all monitors.*

See Also

create, *delete*, *edit*, glob, *list*, *modify*, regex, *show*, *tmsh*

snmp-dca

Configures a Simple Network Management Protocol (SNMP) Data Center Audit monitor.

Syntax

Configure the **snmp** component within the **ltm monitor** module using the syntax in the following sections.

Create/Modify

```
create snmp-dca [name]
modify snmp-dca [name]
    agent-type [generic | other | win2000 | ucd]
    app-service [[string] | none]
    community [ [name] | none]
    cpu-coefficient [ [integer] | none]
    cpu-threshold [none | [integer] ]
    defaults-from [name]
    description [string]
    disk-coefficient [ [integer] | none]
    disk-threshold [none | [integer] ]
    interval [integer]
    memory-coefficient [ [integer] | none]
    memory-threshold [none | [integer] ]
    time-until-up [integer]
    timeout [integer]
    user-defined
    version [ [integer] | none]
edit snmp-dca [ [ [name] | [glob] | [regex] ] ... ]
    all-properties
    non-default-properties
```

Display

```
list snmp-dca
list snmp-dca [ [ [name] | [glob] | [regex] ] ... ]
show snmp-dca [ [ [name] | [glob] | [regex] ] ... ]
show running-config snmp-dca
show running-config snmp-dca [ [ [name] | [glob] | [regex] ] ... ]
    all-properties
    non-default-properties
    one-line
    partition
```

Delete

```
delete snmp-dca [name]
```

◆ Note

You cannot delete default monitors.

Description

You can use the **snmp-dca** component to configure a custom monitor, or you can use the default SNMP DCA monitor that the Local Traffic Manager provides. This type of monitor checks the performance of a server running an SNMP agent such as UC Davis, for the purpose of load balancing traffic to that server.

Examples

create snmp-dca my_snmp-dca defaults-from snmp_dca

Creates a monitor named **my_snmp-dca** that inherits properties from the default SNMP DCA monitor.

list snmp-dca

Displays the properties of all of the SNMP DCA monitors.

Options

- **agent-type**
  Specifies the type of agent. The default value is **ucd**.
- **app-service**
  Specifies the name of the application service to which the monitor belongs. The default value is **none**. **Note:** If the **strict-updates** option is **enabled** on the application service that owns the object, you cannot modify or delete the monitor. Only the application service can modify or delete the monitor.
- **community**
  Specifies the community name that the BIG-IP system must use to authenticate with the host server through SNMP. The default value is **public**.
- **cpu-coefficient**
  Specifies the coefficient that the system uses to calculate the weight of the CPU threshold in the dynamic ratio load balancing algorithm. The default value is **1.5**.
- **cpu-threshold**
  Specifies the maximum acceptable CPU usage on the target server. The default value is **80** percent.
- **defaults-from**
  Specifies the name of the monitor from which you want your custom monitor to inherit settings. The default value is **snmp_dca**.
- **description**
  User defined description.
- **disk-coefficient**
  Specifies the coefficient that the system uses to calculate the weight of the disk threshold in the dynamic ratio load balancing algorithm. The default value is **2.0**.

- **disk-threshold**
  Specifies the maximum acceptable disk usage on the target server. The default value is **90** percent.
- **glob**
  Displays the items that match the **glob** expression. See **help glob** for a description of **glob** expression syntax.
- **interval**
  Specifies the frequency at which the system issues the monitor check. The default value is **10** seconds.
- **memory-coefficient**
  Specifies the coefficient that the system uses to calculate the weight of the memory threshold in the dynamic ratio load balancing algorithm. The default value is **1.0**.
- **memory-threshold**
  Specifies the maximum acceptable memory usage on the target server. The default value is **70** percent.
- **name**
  Specifies a unique name for the component. This option is required for the commands **create**, **delete**, and **modify**.
- **partition**
  Displays the administrative partition within which the component resides.
- **regex**
  Displays the items that match the regular expression. The regular expression must be preceded by an at sign (@[regular expression]) to indicate that the identifier is a regular expression. See **help regex** for a description of regular expression syntax.
- **time-until-up**
  Specifies the amount of time, in seconds, after the first successful response before a node is marked **up**. A value of **0** (zero) causes a node to be marked **up** immediately after a valid response is received from the node. The default value is **0** (zero).
- **timeout**
  Specifies the number of seconds the target has in which to respond to the monitor request. The default value is **30** seconds.
  If the target responds within the set time period, it is considered **up**. If the target does not respond within the set time period, it is considered **down**. Also, if the target responds with a RESET packet, the system immediately flags the target as **down** without waiting for the timeout interval to expire.
- **user-defined**
  Specifies attributes for a monitor that you define. The default value is **none**.
- **version**
  Specifies the version of SNMP that the host server uses. The default value is **none**.

See Also

create, *delete*, *edit*, glob, *list*, *modify*, regex, *show*, *tmsh*

snmp-dca-base

Configures a base Simple Network Management Protocol (SNMP) Data Center Audit monitor.

Syntax

Configure the **snmp-dca-base** component within the **ltm monitor** module using the syntax in the following sections.

Create/Modify

```
create snmp-dca-base [name]
modify snmp-dca-base [name]
    app-service [[string] | none]
    community [ [name] | none]
    cpu-coefficient [ [integer] | none]
    defaults-from [name]
    description [string]
    interval [integer]
    time-until-up [integer]
    timeout [integer]
    user-defined [ [name] [value] | [name] none ]
    version [ [integer] | none]
edit snmp-dca-base [ [ [name] | [glob] | [regex] ] ... ]
    all-properties
    non-default-properties
```

Display

```
list snmp-dca-base
list snmp-dca-base [ [ [name] | [glob] | [regex] ] ... ]
show snmp-dca-base [ [ [name] | [glob] | [regex] ] ... ]
show running-config snmp-dca-base
show running-config snmp-dca-base [ [ [name] | [glob] | [regex] ] ... ]
    all-properties
    non-default-properties
    one-line
    partition
```

Delete

```
delete snmp-dca-base [name]
```

◆ Note

You cannot delete default monitors.

Description

You can use the **snmp-dca-base** component to configure a custom monitor, or you can use the default base SNMP DCA monitor that the Local Traffic Manager provides. This type of monitor checks the performance of a server running an SNMP agent such as UC Davis. Use this monitor only when you want the load balancing destination to be based solely on user data, and not CPU, memory or disk use.

Examples

create snmp-dca-base my_snmp-dca-base defaults-from snmp_dca_base

Creates a monitor named **my_snmp-dca-base** that inherits properties from the default base SNMP DCA monitor.

list snmp-dca-base

Displays the properties of all of the base SNMP DCA monitors.

Options

- **app-service**
  Specifies the name of the application service to which the monitor belongs. The default value is **none**. **Note:** If the **strict-updates** option is **enabled** on the application service that owns the object, you cannot modify or delete the monitor. Only the application service can modify or delete the monitor.
- **community**
  Specifies the community name that the BIG-IP system must use to authenticate with the host server through SNMP. The default value is **public**.
- **defaults-from**
  Specifies the name of the monitor from which you want your custom monitor to inherit settings. The default value is **snmp_dca_base**.
- **description**
  User defined description.
- **glob**
  Displays the items that match the **glob** expression. See **help glob** for a description of **glob** expression syntax.
- **interval**
  Specifies the frequency at which the system issues the monitor check. The default value is **10** seconds.
- **name**
  Specifies a unique name for the component. This option is required for the commands **create**, **delete**, and **modify**.

- **partition**
  Displays the administrative partition within which the component resides.
- **regex**
  Displays the items that match the regular expression. The regular expression must be preceded by an at sign (@[regular expression]) to indicate that the identifier is a regular expression. See **help regex** for a description of regular expression syntax.
- **time-until-up**
  Specifies the amount of time, in seconds, after the first successful response before a node is marked **up**. A value of **0** (zero) causes a node to be marked **up** immediately after a valid response is received from the node. The default value is **0** (zero).
- **timeout**
  Specifies the number of seconds the target has in which to respond to the monitor request. The default value is **30** seconds.
  If the target responds within the set time period, it is considered **up**. If the target does not respond within the set time period, it is considered **down**. Also, if the target responds with a RESET packet, the system immediately flags the target as **down** without waiting for the timeout interval to expire.
- **user-defined**
  Specifies any user-defined command-line arguments and variables that the external program requires. Use the following syntax to specify a user defined parameter.

modify external my_external user-defined my_param_name my_param_value

Use the following syntax to remove a user defined parameter.

modify external my_external user-defined my_param_name none

- **version**
  Specifies the version of SNMP that the host server uses. The default value is **none**.

See Also

create, *delete*, *edit*, glob, *list*, *modify*, regex, *show*, *tmsh*

soap

Configures a Simple Object Access Protocol (SOAP) monitor.

Syntax

Configure the **soap** component within the **ltm monitor** module using the syntax in the following sections.

Create/Modify

```
create soap [name]
modify soap [name]
    app-service [[string] | none]
    debug [no | yes]
    defaults-from [name]
    description [string]
    destination [ip address][port]
    expect-fault [no | yes]
    interval [integer]
    manual-resume [enabled | disabled]
    method [string]
    namespace [ [name] | none]
    parameter-name [ [name] | none]
    parameter-type [bool | int | long | string ]
    parameter-value [none | [integer] | [string] ]
    password [none | [password] ]
    protocol [http | https]
    return-type [bool | char | double | int | long | short | string]
    return-value [none | [integer] | [string] ]
    soap-action [string]
    time-until-up [integer]
    timeout [integer]
    up-interval [integer]
    url-path [none | [string] ]
    username [[name] | none]
edit soap [ [ [name] | [glob] | [regex] ] ... ]
    all-properties
    non-default-properties
```

Display

```
list soap
list soap [ [ [name] | [glob] | [regex] ] ... ]
show soap [ [ [name] | [glob] | [regex] ] ... ]
show running-config soap
show running-config soap [ [ [name] | [glob] | [regex] ] ... ]
    all-properties
    non-default-properties
    one-line
    partition
```

Delete

```
delete soap [name]
```

◆ Note

You cannot delete default monitors.

Description

You can use the **soap** component to configure a custom monitor, or you can use the default SOAP monitor that the Local Traffic Manager provides. This type of monitor tests a Web service based on SOAP.

Examples

create soap my_soap defaults-from soap

Creates a **soap** monitor that inherits values from the system default SOAP monitor.

list soap

Displays the properties of all of the SOAP monitors.

Options

- **app-service**
  Specifies the name of the application service to which the monitor belongs. The default value is **none**. **Note:** If the **strict-updates** option is **enabled** on the application service that owns the object, you cannot modify or delete the monitor. Only the application service can modify or delete the monitor.
- **debug**
  Specifies whether the monitor sends error messages and additional information to a log file created and labeled specifically for this monitor. You can use the log information to help diagnose and troubleshoot unsuccessful health checks. The default value is **no**.
  The options are:
  - **no**
    Specifies that the system does not redirect error messages and additional information related to this monitor.
  - **yes**
    Specifies that the system redirects error messages and additional information to the /var/log/monitors/<monitor_name>-<node_name>-<port>.log file.
- **defaults-from**
  Specifies the type of monitor you want to use to create the new monitor. The default value is **soap**.

- **description**
  User defined description.
- **destination**
  Specifies the IP address and service port of the resource that is the destination of this monitor. Possible values are:
  - ***:***
    Specifies to perform a health check on the IP address and port supplied by a pool member.
  - ***:port**
    Specifies to perform a health check on the server with the IP address supplied by the pool member and the port you specify.
  - **IP address:port**
    Specifies to mark a pool member **up** or **down** based on the response of the server at the IP address and port you specify.
- **expect-fault**
  Specifies whether the value of the **method** option causes the monitor to expect a SOAP fault message. The default value is **no**.
- **glob**
  Displays the items that match the **glob** expression. See **help glob** for a description of **glob** expression syntax.
- **interval**
  Specifies, in seconds, the frequency at which the system issues the monitor check when either the resource is **down** or the status of the resource is unknown. The default value is **5** seconds.

*F5 Networks recommends that when you configure this option and the **up-interval** option, whichever value is greater be a multiple of the lesser value to allow for an even distribution of monitor checks among all monitors.*

- **manual-resume**
  Specifies whether the system automatically changes the status of a resource to **up** at the next successful monitor check. The default value of the manual-resume option is **disabled**.
  Note that if you set the **manual-resume** option to **enabled**, you must manually mark the resource as **up** before the system can use it for load balancing connections.
- **method**
  Specifies the method by which the monitor contacts the resource.
- **name**
  Specifies a unique name for the component. This option is required for the commands **create**, **delete**, and **modify**.
- **namespace**
  Specifies the name space for the Web service you are monitoring, for example, **http://example.com/**. The default value is **none**.

- **parameter-name**
  If the method has a parameter, specifies the name of that parameter. The default value is **none**.
- **parameter-type**
  Specifies the parameter type. The default value is **bool**.
- **parameter-value**
  Specifies the value for the parameter. The default value is **none**.
- **partition**
  Displays the administrative partition within which the component resides.
- **password**
  Specifies the password if the monitored target requires authentication. The default value is **none**.
- **protocol**
  Specifies the protocol that the monitor uses to communicate with the target, **http** or **https**. The default value is **http**.
- **regex**
  Displays the items that match the regular expression. The regular expression must be preceded by an at sign (@[regular expression]) to indicate that the identifier is a regular expression. See **help regex** for a description of regular expression syntax.
- **return-type**
  Specifies the type for the returned parameter. The default value is **bool**.
- **return-value**
  Specifies the value for the returned parameter. The default value is **none**.
- **soap-action**
  Specifies the value for the SOAPAction header. The default value is the empty string.
- **time-until-up**
  Specifies the amount of time, in seconds, after the first successful response before a node is marked **up**. A value of **0** (zero) causes a node to be marked **up** immediately after a valid response is received from the node. The default value is **0** (zero).
- **timeout**
  Specifies the number of seconds the target has in which to respond to the monitor request. The default value is **16** seconds. If the target responds within the set time period, it is considered up. If the target does not respond within the set time period, it is considered down. Also, if the target responds with a RESET packet, the system immediately flags the target as down without waiting for the timeout interval to expire.
- **url-path**
  Specifies the URL for the Web service that you are monitoring, for example, **/services/myservice.aspx**. The default value is **none**.

- **up-interval**
  Specifies, in seconds, the frequency at which the system issues the monitor check when the resource is **up**. The default value is **0** (zero), which specifies that the system uses the value of the **interval** option whether the resource is **up** or **down**.

Important

*F5 Networks recommends that when you configure this option and the **interval** option, whichever value is greater be a multiple of the lesser value to allow for an even distribution of monitor checks among all monitors.*

- **username**
  Specifies the user name if the monitored target requires authentication. The default value is **none**.

See Also

create, *delete*, *edit*, glob, *list*, *modify*, regex, *show*, *tmsh*

tcp

Configures a Transmission Control Protocol (TCP) monitor.

Syntax

Configure the **tcp** component within the **ltm monitor** module using the syntax in the following sections.

Create/Modify

```
create tcp [name]
modify tcp [name]
    adaptive [enabled | disabled]
    adaptive-divergence-type [relative | absolute]
    adaptive-divergence-value [integer]
    adaptive-limit [integer]
    adaptive-sampling-timespan [integer]
    app-service [[string] | none]
    defaults-from [name]
    description [string]
    destination [ip address][port]
    interval [integer]
    ip-dscp [integer]
    manual-resume [enabled | disabled]
    recv [none | [string] ]
    recv-disable [none | [string] ]
    reverse [enabled | disabled]
    send [none | [string] ]
    time-until-up [integer]
    timeout [integer]
    transparent [disabled | enabled]
    up-interval [integer]
edit tcp [ [ [name] | [glob] | [regex] ] ... ]
    all-properties
    non-default-properties
```

Display

```
list tcp
list tcp [ [ [name] | [glob] | [regex] ] ... ]
show tcp [ [ [name] | [glob] | [regex] ] ... ]
show running-config tcp
show running-config tcp [ [ [name] | [glob] | [regex] ] ... ]
    all-properties
    non-default-properties
    one-line
    partition
```

Delete

```
delete tcp [name]
```

◆ Note

You cannot delete default monitors.

Description

You can use the **tcp** component to configure a custom monitor, or you can use the default TCP monitor that the Local Traffic Manager provides.

Examples

create tcp my_tcp defaults-from tcp

Creates a monitor named **my_tcp** that inherits properties from the default TCP monitor.

list tcp

Displays the properties of all of the TCP monitors.

Options

- **adaptive**
  Specifies whether the adaptive feature is enabled for this monitor. Not all monitors support the adaptive feature.
- **adaptive-divergence-type**
  Specifies whether the *adaptive-divergence-value* is **relative** or **absolute**.
- **adaptive-divergence-value**
  Specifies how far from mean latency each monitor probe is allowed to be. If *adaptive-divergence-type* is *relative*, this value is a percentage deviation from mean (e.g. 50 would indicate the probe is allowed to exceed the mean latency by 50%.) If *adaptive-divergence-type* is *absolute*, this value is an offset from mean in milliseconds (e.g. 250 would indicate the probe is allowed allowed to exceed the mean latency by 250 ms.) A probe that exceeds latency is counted the same as a probe that is not received, so in the typical scenario, it will require three missed latencies in a row to mark a pool member or node down (i.e. a 15-second interval with a 46-second timeout, would require three missed probes before the pool member or node would be marked down.)
- **adaptive-limit**
  Specifies the hard limit, in milliseconds, which the probe is not allowed to exceed, regardless of the divergence value. For example, if this value is 500, then the probe latency may not exceed 500 ms even if that would still fall within the divergence value.

- **adaptive-sampling-timespan**
  Specifies the size of the sliding window, in seconds, which records probe history. For example, if this value is 300, then a sliding window of the last five minutes' probe history will be used for calculating probe mean latency and standard deviation.
- **app-service**
  Specifies the name of the application service to which the monitor belongs. The default value is **none**. **Note:** If the **strict-updates** option is **enabled** on the application service that owns the object, you cannot modify or delete the monitor. Only the application service can modify or delete the monitor.
- **defaults-from**
  Specifies the name of the monitor from which you want your custom monitor to inherit settings. The default value is **tcp**.
- **description**
  User defined description.
- **destination**
  Specifies the IP address and service port of the resource that is the destination of this monitor. The default value is ***:***.
  Possible values are:
  - ***:***
    Specifies to perform a health check on the IP address and port supplied by a pool member.
  - ***:port**
    Specifies to perform a health check on the server with the IP address supplied by the pool member and the port you specify.
  - **IP address:port**
    Specifies to mark a pool member **up** or **down** based on the response of the server at the IP address and port you specify.
  - **IP address:port** (with the **transparent** option **enabled**)
    Specifies to perform a health check on the server at the IP address and port you specify, route the check through the IP address and port supplied by the pool member, and mark the pool member (the gateway) **up** or **down** accordingly.
- **glob**
  Displays the items that match the **glob** expression. See **help glob** for a description of **glob** expression syntax.
- **interval**
  Specifies, in seconds, the frequency at which the system issues the monitor check when either the resource is **down** or the status of the resource is unknown. The default value is **5** seconds.

Important

*F5 Networks recommends that when you configure this option and the **up-interval** option, whichever value is greater be a multiple of the lesser value to allow for an even distribution of monitor checks among all monitors.*

- **ip-dscp**
  Specifies the differentiated services code point (DSCP). DSCP is a 6-bit value in the Differentiated Services (DS) field of the IP header. It can be used to specify the quality of service desired for the packet. The valid range for this value is 0 to 63 (hex 0x0 to 0x3f). The default value is zero.
- **manual-resume**
  Specifies whether the system automatically changes the status of a resource to **up** at the next successful monitor check. The default value of the manual-resume option is **disabled**.
  Note that if you set the **manual-resume** option to **enabled**, you must manually mark the resource as **up** before the system can use it for load balancing connections.
- **name**
  Specifies a unique name for the component. This option is required for the commands **create**, **delete**, and **modify**.
- **partition**
  Displays the administrative partition within which the component resides.
- **recv**
  Specifies the text string that the monitor looks for in the returned resource. The default value is **none**.
  The most common receive expressions contain a text string that is included in an HTML file on your site. The text string can be regular text, HTML tags, or image names. If you do not specify a value for both the **send** and **recv** options, the monitor performs a simple service check and connect only.
- **recv-disable**
  Specifies a text string that the monitor looks for in the returned resource. If the text string is matched in the returned resource, the corresponding node or pool member is marked session disabled. The default value is **none**.
  You specify a **recv-disable** string in the same way that you specify a **recv** string.
  If you specify a **recv-disable** string, you must also specify a **recv** string. You cannot specify a **recv-disable** string, if the **reverse** option is **enabled**.
- **regex**
  Displays the items that match the regular expression. The regular expression must be preceded by an at sign (@[regular expression]) to indicate that the identifier is a regular expression. See **help regex** for a description of regular expression syntax.
- **reverse**
  Specifies whether the monitor operates in reverse mode. When the monitor is in reverse mode, a successful check marks the monitored object **down** instead of **up**. You can use the this mode only if you configure both the **send** and **recv** options.
  The default value is **disabled**, which specifies that the monitor does not operate in reverse mode. The **enabled** value specifies that the monitor operates in reverse mode.

- **send**
  Specifies the text string that the monitor sends to the target object. The default setting is **GET /**, which retrieves a default HTML file for a web site.
  To retrieve a specific page from a web site, specify a fully-qualified path name, for example, **GET /www/company/index.html**. Since the string may have special characters, the system may require that the string be enclosed with single quotation marks.
  If this value is null, then a valid connection suffices to determine that the service is **up**. In this case, the system does not need the recv option and ignores the option even if not null.
- **time-until-up**
  Specifies the amount of time, in seconds, after the first successful response before a node is marked **up**. A value of **0** (zero) causes a node to be marked **up** immediately after a valid response is received from the node. The default value is **0** (zero).
- **timeout**
  Specifies the number of seconds the target has in which to respond to the monitor request. The default value is **16** seconds.
  If the target responds within the set time period, it is considered **up**. If the target does not respond within the set time period, it is considered **down**. Also, if the target responds with a RESET packet, the system immediately flags the target as **down** without waiting for the timeout interval to expire.
- **transparent**
  Specifies whether the monitor operates in transparent mode. Monitors in transparent mode can monitor pool members through firewalls. The default value is **disabled**.
- **up-interval**
  Specifies, in seconds, the frequency at which the system issues the monitor check when the resource is **up**. The default value is **0** (zero), which specifies that the system uses the value of the **interval** option whether the resource is **up** or **down**.

Important

*F5 Networks recommends that when you configure this option and the **interval** option, whichever value is greater be a multiple of the lesser value to allow for an even distribution of monitor checks among all monitors.*

See Also

create, *delete*, *edit*, glob, *list*, *modify*, regex, *show*, *tmsh*

tcp-echo

Configures a Transmission Control Protocol (TCP) Echo monitor.

Syntax

Configure the **tcp-echo** component within the **ltm monitor** module using the syntax in the following sections.

Create/Modify

```
create tcp-echo [name]
modify tcp-echo [name]
    adaptive [enabled | disabled]
    adaptive-divergence-type [relative | absolute]
    adaptive-divergence-value [integer]
    adaptive-limit [integer]
    adaptive-sampling-timespan [integer]
    app-service [[string] | none]
    defaults-from [name]
    description [string]
    destination [ip address]
    interval [integer]
    manual-resume [enabled | disabled]
    time-until-up [integer]
    timeout [integer]
    transparent [disabled | enabled]
    up-interval [integer]
edit tcp-echo [ [ [name] | [glob] | [regex] ] ... ]
    all-properties
    non-default-properties
```

Display

```
list tcp
list tcp [ [ [name] | [glob] | [regex] ] ... ]
show tcp [ [ [name] | [glob] | [regex] ] ... ]
show running-config tcp-echo
show running-config tcp-echo [ [ [name] | [glob] | [regex] ] ... ]
    all-properties
    non-default-properties
    one-line
    partition
```

Delete

```
delete tcp-echo [name]
```

◆ Note

You cannot delete default monitors.

Description

You can use the **tcp-echo** component to configure a custom monitor, or you can use the default TCP Echo monitor that the Local Traffic Manager provides. This type of monitor checks the status of a resource, using TCP Echo.

Examples

create tcp-echo my_tcp-echo defaults-from tcp_echo

Creates a monitor named **my_tcp-echo** that inherits properties from the default TCP Echo monitor.

list tcp-echo

Displays the properties of all of the TCP Echo monitors.

Options

- **adaptive**
  Specifies whether the adaptive feature is enabled for this monitor. Not all monitors support the adaptive feature.
- **adaptive-divergence-type**
  Specifies whether the *adaptive-divergence-value* is **relative** or **absolute**.
- **adaptive-divergence-value**
  Specifies how far from mean latency each monitor probe is allowed to be. If *adaptive-divergence-type* is *relative*, this value is a percentage deviation from mean (e.g. 50 would indicate the probe is allowed to exceed the mean latency by 50%.) If *adaptive-divergence-type* is *absolute*, this value is an offset from mean in milliseconds (e.g. 250 would indicate the probe is allowed allowed to exceed the mean latency by 250 ms.) A probe that exceeds latency is counted the same as a probe that is not received, so in the typical scenario, it will require three missed latencies in a row to mark a pool member or node down (i.e. a 15-second interval with a 46-second timeout, would require three missed probes before the pool member or node would be marked down.)
- **adaptive-limit**
  Specifies the hard limit, in milliseconds, which the probe is not allowed to exceed, regardless of the divergence value. For example, if this value is 500, then the probe latency may not exceed 500 ms even if that would still fall within the divergence value.
- **adaptive-sampling-timespan**
  Specifies the size of the sliding window, in seconds, which records probe history. For example, if this value is 300, then a sliding window of the last five minutes' probe history will be used for calculating probe mean latency and standard deviation.

- **app-service**
  Specifies the name of the application service to which the monitor belongs. The default value is **none**. **Note:** If the **strict-updates** option is **enabled** on the application service that owns the object, you cannot modify or delete the monitor. Only the application service can modify or delete the monitor.
- **defaults-from**
  Specifies the name of the monitor from which you want your custom monitor to inherit settings. The default value is **tcp_echo**.
- **description**
  User defined description.
- **destination**
  Specifies the IP address of the resource that is the destination of this monitor. The default value is *****.
  Possible values are:
  - *****
    Specifies to perform a health check on the IP address of the node.
  - **IP address**
    Specifies to perform a health check on the IP address that you specify, and mark the associated node **up** or **down** accordingly.
  - **IP address** (with the **transparent** option **enabled**)
    Specifies to perform a health check on the IP address that you specify, route the check through the IP address of the associated node, and mark the IP address of the associated node **up** or **down** accordingly.
- **glob**
  Displays the items that match the **glob** expression. See **help glob** for a description of **glob** expression syntax.
- **interval**
  Specifies, in seconds, the frequency at which the system issues the monitor check when either the resource is **down** or the status of the resource is unknown. The default value is **5** seconds.

Important

*F5 Networks recommends that when you configure this option and the **up-interval** option, whichever value is greater be a multiple of the lesser value to allow for an even distribution of monitor checks among all monitors.*

- **manual-resume**
  Specifies whether the system automatically changes the status of a resource to **up** at the next successful monitor check. The default value of the manual-resume option is **disabled**.
  Note that if you set the **manual-resume** option to **enabled**, you must manually mark the resource as **up** before the system can use it for load balancing connections.
- **name**
  Specifies a unique name for the component. This option is required for the commands **create**, **delete**, and **modify**.

- **partition**
  Displays the administrative partition within which the component resides.
- **regex**
  Displays the items that match the regular expression. The regular expression must be preceded by an at sign (@[regular expression]) to indicate that the identifier is a regular expression. See **help regex** for a description of regular expression syntax.
- **time-until-up**
  Specifies the amount of time, in seconds, after the first successful response before a node is marked **up**. A value of **0** (zero) causes a node to be marked **up** immediately after a valid response is received from the node. The default value is **0** (zero).
- **timeout**
  Specifies the number of seconds the target has in which to respond to the monitor request. The default value is **16** seconds.
  If the target responds within the set time period, it is considered **up**. If the target does not respond within the set time period, it is considered **down**. Also, if the target responds with a RESET packet, the system immediately flags the target as **down** without waiting for the timeout interval to expire.
- **transparent**
  Specifies whether the monitor operates in transparent mode. Monitors in transparent mode can monitor pool members through firewalls. The default value is **disabled**.
- **up-interval**
  Specifies, in seconds, the frequency at which the system issues the monitor check when the resource is **up**. The default value is **0** (zero), which specifies that the system uses the value of the **interval** option whether the resource is **up** or **down**.

Important

*F5 Networks recommends that when you configure this option and the **interval** option, whichever value is greater be a multiple of the lesser value to allow for an even distribution of monitor checks among all monitors.*

See Also

create, *delete*, *edit*, glob, *list*, *modify*, regex, *show*, *tmsh*

tcp-half-open

Configures a Transmission Control Protocol (TCP) Half Open monitor.

Syntax

Configure the **tcp-half-open** component within the **ltm monitor** module using the syntax in the following sections.

Create/Modify

```
create tcp-half-open [name]
modify tcp-half-open [name]
    app-service [[string] | none]
    defaults-from [name]
    description [string]
    destination [ip address][port]
    interval [integer]
    manual-resume [enabled | disabled]
    time-until-up [integer]
    timeout [integer]
    transparent [disabled | enabled]
    up-interval [integer]
edit tcp-half-open [ [ [name] | [glob] | [regex] ] ... ]
    all-properties
    non-default-properties
```

Display

```
list tcp-half-open
list tcp-half-open [ [ [name] | [glob] | [regex] ] ... ]
show tcp-half-open [ [ [name] | [glob] | [regex] ] ... ]
show running-config tcp-half-open
show running-config tcp-half-open [ [ [name] | [glob] |
                                      [regex] ] ... ]
    all-properties
    non-default-properties
    one-line
    partition
```

Delete

```
delete tcp-half-open [name]
```

◆ Note

You cannot delete default monitors.

Description

You can use the **tcp-half-open** component to configure a custom monitor, or you can use the default TCP Half Open monitor that the Local Traffic Manager provides.

For more information about configuring monitors, refer to the *Configuration Guide for BIG-IP® Local Traffic Manager®*.

Examples

create tcp-half-open my_tcp-half-open defaults-from tcp_half_open

Creates a monitor named **my_tcp-half-open** that inherits properties from the default TCP Half Open monitor.

list tcp-half-open

Displays the properties of all of the TCP Half Open monitors.

Options

- **app-service**
  Specifies the name of the application service to which the monitor belongs. The default value is **none**. **Note:** If the **strict-updates** option is **enabled** on the application service that owns the object, you cannot modify or delete the monitor. Only the application service can modify or delete the monitor.
- **defaults-from**
  Specifies the name of the monitor from which you want your custom monitor to inherit settings. The default value is **tcp_half_open**.
- **description**
  User defined description.
- **destination**
  Specifies the IP address and service port of the resource that is the destination of this monitor. The default value is ***:***.
  Possible values are:
  - ***:***
    Specifies to perform a health check on the IP address and port supplied by a pool member.
  - ***:port**
    Specifies to perform a health check on the server with the IP address supplied by the pool member and the port you specify.
  - **IP address:port**
    Specifies to mark a pool member **up** or **down** based on the response of the server at the IP address and port you specify.

- **IP address:port** (with the **transparent** option **enabled**)
  Specifies to perform a health check on the server at the IP address and port you specify, route the check through the IP address and port supplied by the pool member, and mark the pool member (the gateway) **up** or **down** accordingly.

- **glob**
  Displays the items that match the **glob** expression. See **help glob** for a description of **glob** expression syntax.
- **interval**
  Specifies, in seconds, the frequency at which the system issues the monitor check when either the resource is **down** or the status of the resource is unknown. The default value is **5** seconds.

Important

*F5 Networks recommends that when you configure this option and the **up-interval** option, whichever value is greater be a multiple of the lesser value to allow for an even distribution of monitor checks among all monitors.*

- **manual-resume**
  Specifies whether the system automatically changes the status of a resource to **up** at the next successful monitor check. The default value of the manual-resume option is **disabled**.
  Note that if you set the **manual-resume** option to **enabled**, you must manually mark the resource as **up** before the system can use it for load balancing connections.
- **name**
  Specifies a unique name for the component. This option is required for the commands **create**, **delete**, and **modify**.
- **partition**
  Displays the administrative partition within which the component resides.
- **regex**
  Displays the items that match the regular expression. The regular expression must be preceded by an at sign (@[regular expression]) to indicate that the identifier is a regular expression. See **help regex** for a description of regular expression syntax.
- **time-until-up**
  Specifies the amount of time, in seconds, after the first successful response before a node is marked **up**. A value of **0** (zero) causes a node to be marked **up** immediately after a valid response is received from the node. The default value is **0** (zero).
- **timeout**
  Specifies the number of seconds the target has in which to respond to the monitor request. The default value is **16** seconds.
  If the target responds within the set time period, it is considered **up**. If the target does not respond within the set time period, it is considered **down**.

Also, if the target responds with a RESET packet, the system immediately flags the target as **down** without waiting for the timeout interval to expire.

- **transparent**
  Specifies whether the monitor operates in transparent mode. Monitors in transparent mode can monitor pool members through firewalls. The default value is **disabled**.
- **up-interval**
  Specifies, in seconds, the frequency at which the system issues the monitor check when the resource is **up**. The default value is **0** (zero), which specifies that the system uses the value of the **interval** option whether the resource is **up** or **down**.

Important

*F5 Networks recommends that when you configure this option and the **interval** option, whichever value is greater be a multiple of the lesser value to allow for an even distribution of monitor checks among all monitors.*

See Also

create, *delete*, *edit*, glob, *list*, *modify*, regex, *show*, *tmsh*

udp

Configures a User Datagram Protocol (UDP) monitor.

Syntax

Configure the **udp** component within the **ltm monitor** module using the syntax in the following sections.

Create/Modify

```
create udp [name]
modify udp [name]
    adaptive [enabled | disabled]
    adaptive-divergence-type [relative | absolute]
    adaptive-divergence-value [integer]
    adaptive-limit [integer]
    adaptive-sampling-timespan [integer]
    app-service [[string] | none]
    debug [no | yes]
    defaults-from [name]
    description [string]
    destination [ip address][port]
    interval [integer]
    manual-resume [enabled | disabled]
    recv [none | [string] ]
    recv-disable [none | [string] ]
    reverse [enabled | disabled]
    send [none | [string] ]
    time-until-up [integer]
    timeout [integer]
    transparent [disabled | enabled]
    up-interval [integer]
edit udp [ [ [name] | [glob] | [regex] ] ... ]
    all-properties
    non-default-properties
```

Display

```
list udp
list udp [ [ [name] | [glob] | [regex] ] ... ]
show udp [ [ [name] | [glob] | [regex] ] ... ]
show running-config udp
show running-config udp [ [ [name] | [glob] | [regex] ] ... ]
    all-properties
    non-default-properties
    one-line
    partition
```

Delete

```
delete udp [name]
```

◆ Note

You cannot delete default monitors.

Description

You can use the **udp** component to configure a custom monitor, or you can use the default UDP monitor that the Local Traffic Manager provides. This type of monitor verifies the UDP service by attempting to send UDP packets to a pool, pool member, or virtual server and receiving a reply.

Examples

create udp my_udp defaults-from udp

Creates a monitor named **my_udp** that inherits properties from the default UDP monitor.

list udp

Displays the properties of all of the UDP monitors.

Options

- **adaptive**
  Specifies whether the adaptive feature is enabled for this monitor. Not all monitors support the adaptive feature.
- **adaptive-divergence-type**
  Specifies whether the *adaptive-divergence-value* is **relative** or **absolute**.
- **adaptive-divergence-value**
  Specifies how far from mean latency each monitor probe is allowed to be. If *adaptive-divergence-type* is *relative*, this value is a percentage deviation from mean (e.g. 50 would indicate the probe is allowed to exceed the mean latency by 50%.) If *adaptive-divergence-type* is *absolute*, this value is an offset from mean in milliseconds (e.g. 250 would indicate the probe is allowed allowed to exceed the mean latency by 250 ms.) A probe that exceeds latency is counted the same as a probe that is not received, so in the typical scenario, it will require three missed latencies in a row to mark a pool member or node down (i.e. a 15-second interval with a 46-second timeout, would require three missed probes before the pool member or node would be marked down.)

- **adaptive-limit**
  Specifies the hard limit, in milliseconds, which the probe is not allowed to exceed, regardless of the divergence value. For example, if this value is 500, then the probe latency may not exceed 500 ms even if that would still fall within the divergence value.
- **adaptive-sampling-timespan**
  Specifies the size of the sliding window, in seconds, which records probe history. For example, if this value is 300, then a sliding window of the last five minutes' probe history will be used for calculating probe mean latency and standard deviation.
- **app-service**
  Specifies the name of the application service to which the monitor belongs. The default value is **none**. **Note:** If the **strict-updates** option is **enabled** on the application service that owns the object, you cannot modify or delete the monitor. Only the application service can modify or delete the monitor.
- **debug**
  Specifies whether the monitor sends error messages and additional information to a log file created and labeled specifically for this monitor. You can use the log information to help diagnose and troubleshoot unsuccessful health checks. The default value is **no**.
  The options are:
  - **no**
    Specifies that the system does not redirect error messages and additional information related to this monitor.
  - **yes**
    Specifies that the system redirects error messages and additional information to the /var/log/monitors/<monitor_name>-<node_name>-<port>.log file.
- **defaults-from**
  Specifies the name of the monitor from which you want your custom monitor to inherit settings. The default value is **udp**.
- **description**
  User defined description.
- **destination**
  Specifies the IP address and service port of the resource that is the destination of this monitor. Possible values are:
  - ***:***
    Specifies to perform a health check on the IP address and port supplied by a pool member.
  - ***:port**
    Specifies to perform a health check on the server with the IP address supplied by the pool member and the port you specify.
  - **IP address:port**
    Specifies to mark a pool member **up** or **down** based on the response of the server at the IP address and port you specify.

- **IP address:port** (with the **transparent** option **enabled**)
  Specifies to perform a health check on the server at the IP address and port you specify, route the check through the IP address and port supplied by the pool member, and mark the pool member (the gateway) **up** or **down** accordingly.

- **glob**
  Displays the items that match the **glob** expression. See **help glob** for a description of **glob** expression syntax.

- **interval**
  Specifies, in seconds, the frequency at which the system issues the monitor check when either the resource is **down** or the status of the resource is unknown. The default value is **5** seconds.

Important

*F5 Networks recommends that when you configure this option and the **up-interval** option, whichever value is greater be a multiple of the lesser value to allow for an even distribution of monitor checks among all monitors.*

- **manual-resume**
  Specifies whether the system automatically changes the status of a resource to **up** at the next successful monitor check. The default value of the manual-resume option is **disabled**.
  Note that if you set the **manual-resume** option to **enabled**, you must manually mark the resource as **up** before the system can use it for load balancing connections.

- **name**
  Specifies a unique name for the component. This option is required for the commands **create**, **delete**, and **modify**.

- **partition**
  Displays the administrative partition within which the component resides.

- **recv**
  Specifies the text string that the monitor looks for in the returned resource. The default value is **none**.

- **recv-disable**
  Specifies a text string that the monitor looks for in the returned resource. If the text string is matched in the returned resource, the corresponding node or pool member is marked session disabled. The default value is **none**.
  The **recv-disable** string may be specified the same way a **recv** string may be specified.
  If the **recv-disable** string is configured, the recv string must be non-empty. The **recv-disable** string may not be configured if **reverse** mode is enabled.

- **regex**
  Displays the items that match the regular expression. The regular expression must be preceded by an at sign (@[regular expression]) to indicate that the identifier is a regular expression. See **help regex** for a description of regular expression syntax.
- **reverse**
  Specifies whether the monitor operates in reverse mode. When the monitor is in reverse mode, a successful check marks the monitored object **down** instead of **up**. You can use the this mode only if you configure both the **send** and **recv** options.
  The default value is **disabled**, which specifies that the monitor does not operate in reverse mode. The **enabled** value specifies that the monitor operates in reverse mode.
- **send**
  Specifies the text string that the monitor sends to the target object. The default value is **GET /**, which retrieves a default HTML file for a web site.
  To retrieve a specific page from a web site, specify a fully-qualified path name, for example, **GET /www/company/index.html**. Since the string may have special characters, the system may require that the string be enclosed with single quotation marks.
  If this value is null, then a valid connection suffices to determine that the service is **up**. In this case, the system does not need the **recv** option and ignores the option even if it is not null. The default value is **none**.
- **time-until-up**
  Specifies the amount of time, in seconds, after the first successful response before a node is marked **up**. A value of **0** (zero) causes a node to be marked **up** immediately after a valid response is received from the node. The default value is **0** (zero).
- **timeout**
  Specifies the number of seconds the target has in which to respond to the monitor request. The default value is **16** seconds. If the target responds within the set time period, it is considered up. If the target does not respond within the set time period, it is considered down. Also, if the target responds with a RESET packet, the system immediately flags the target as down without waiting for the timeout interval to expire.
- **transparent**
  Specifies whether the monitor operates in transparent mode. Monitors in transparent mode can monitor pool members through firewalls. The default value is **disabled**.

- **up-interval**
  Specifies, in seconds, the frequency at which the system issues the monitor check when the resource is **up**. The default value is **0** (zero), which specifies that the system uses the value of the **interval** option whether the resource is **up** or **down**.

Important

*F5 Networks recommends that when you configure this option and the **interval** option, whichever value is greater be a multiple of the lesser value to allow for an even distribution of monitor checks among all monitors.*

See Also

create, *delete*, *edit*, glob, *list*, *modify*, regex, *show*, *tmsh*

virtual-location

Configures a Virtual Location monitor.

Syntax

Configure the **virtual-location** component within the **ltm monitor** module using the syntax shown in the following sections.

Create/Modify

```
create virtual-location [name]
modify virtual-location [name]
    app-service [[string] | none]
    debug [no | yes]
    defaults-from [name]
    description [string]
    interval [integer]
    pool [name]
    time-until-up [integer]
    timeout [integer]
    up-interval [integer]
edit virtual-location [ [ [name] | [glob] | [regex] ] ... ]
      all-properties
      non-default-properties
```

Display

```
list virtual-location
list virtual-location [ [ [name] | [glob] | [regex] ] ... ]
show virtual-location [ [ [name] | [glob] | [regex] ] ... ]
show running-config virtual-location
show running-config virtual-location
                     [ [ [name] | [glob] | [regex] ] ... ]
    all-properties
    non-default-properties
    one-line
    partition
```

Delete

```
delete virtual-location [name]
```

◆ Note

You cannot delete default monitors.

Description

The Virtual Location monitor will determine if a pool member which has a virtual IP is currently a local pool member with its arp entry existing on a local VLAN, or, a remote pool member with its ARP entry existing on a

tunnel VLAN. If the pool member is local it will set the pool member's priority to 2. If the pool member is remote it will set the priority to 1 (a lower priority). The Virtual Location will always return up as the availability for the pool member. It is necessary to use an additional monitor to check the availability status of the pool member.

You can use the **virtual-location** component to configure a custom monitor, or you can use the default Virtual Location monitor that the Local Traffic Manager provides.

Examples

create virtual-location my_virtual-location defaults-from virtual_location pool aPool

Creates a monitor named **my_virtual-location** that inherits properties from the default Virtual Location monitor.

list virtual-location

Displays the properties of all of the Virtual Location monitors.

Options

- **app-service**
  Specifies the name of the application service to which the monitor belongs. The default value is **none**. **Note:** If the **strict-updates** option is **enabled** on the application service that owns the object, you cannot modify or delete the monitor. Only the application service can modify or delete the monitor.
- **debug**
  Specifies whether the monitor sends error messages and additional information to a log file created and labeled specifically for this monitor. The default setting is no. You can use the log information to help diagnose and troubleshoot unsuccessful health checks. The options are no (specifies that the system does not redirect error messages and additional information related to this monitor.) and yes (specifies that the system redirects error messages and additional information to the /var/log/monitors/<monitor_name>-<node_name>-<port>.log file.)
- **defaults-from**
  Specifies the name of the monitor from which you want your custom monitor to inherit settings. The default value is **virtual_location**.
- **description**
  User defined description.
- **glob**
  Displays the items that match the **glob** expression. See **help glob** for a description of **glob** expression syntax.

- **interval**
  Specifies, in seconds, the frequency at which the system issues the monitor check when either the resource is **down** or the status of the resource is unknown. The default value is **5** seconds.

Important

*F5 Networks recommends that when you configure this option and the **up-interval** option, whichever value is greater be a multiple of the lesser value to allow for an even distribution of monitor checks among all monitors.*

- **name**
  Specifies a unique name for the component. This option is required for the commands **create**, **delete**, and **modify**.
- **partition**
  Displays the administrative partition within which the component resides.
- **pool**
  Specifies the pool for the target pool member. This is a required argument.
- **regex**
  Displays the items that match the regular expression. The regular expression must be preceded by an at sign (@[regular expression]) to indicate that the identifier is a regular expression. See **help regex** for a description of regular expression syntax.
- **time-until-up**
  Specifies the amount of time, in seconds, after the first successful response before a node is marked **up**. A value of **0** (zero) causes a node to be marked **up** immediately after a valid response is received from the node. The default value is **0** (zero).
- **timeout**
  Specifies the number of seconds the target has in which to respond to the monitor request. The default value is **16** seconds.
  If the target responds within the set time period, it is considered **up**. If the target does not respond within the set time period, it is considered **down**. Also, if the target responds with a RESET packet, the system immediately flags the target as **down** without waiting for the timeout interval to expire.
- **up-interval**
  Specifies, in seconds, the frequency at which the system issues the monitor check when the resource is **up**. The default value is **0** (zero), which specifies that the system uses the value of the **interval** option whether the resource is **up** or **down**.

Important

*F5 Networks recommends that when you configure this option and the **interval** option, whichever value is greater be a multiple of the lesser value to allow for an even distribution of monitor checks among all monitors.*

See Also

create, *delete*, *edit*, glob, *list*, *pool*, *modify*, regex, *tmsh*

wap

Configures a Wireless Application Protocol (WAP) monitor.

Syntax

Configure the **wap** component within the **ltm monitor** module using the syntax in the following sections.

Create/Modify

```
create wap [name]
modify wap [name]
    accounting-node [none | [RADIUS server name] ]
    accounting-port [[integer] | none]
    app-service [[string] | none]
    call-id [none | [RADIUS server 11 digit phone number] ]
    debug [no | yes]
    defaults-from [name]
    description [string]
    destination [ip address][port]
    framed-address [none | [RADIUS framed IP address] ]
    interval [integer]
    manual-resume [enabled | disabled]
    recv [none | [string] ]
    secret [none | [password] ]
    send [none | [string]]
    server-id [none | [RADIUS NAS-ID] ]
    session-id [none | [RADIUS session ID] ]
    time-until-up [integer]
    timeout [integer]
    up-interval [integer]
edit wap [ [ [name] | [glob] | [regex] ] ... ]
    all-properties
    non-default-properties
```

Display

```
list wap
list wap[ [ [name] | [glob] | [regex] ] ... ]
show wap[ [ [name] | [glob] | [regex] ] ... ]
show running-config wap
show running-config wap [ [ [name] | [glob] | [regex] ] ... ]
    all-properties
    non-default-properties
    one-line
    partition
```

Delete

```
delete wap [name]
```

◆ Note

You cannot delete default monitors.

Description

You can use the **wap** component to configure a custom monitor, or you can use the default WAP monitor that the Local Traffic Manager provides. This type of monitor requests the URL specified in the send option, and finds the string specified in the recv option somewhere in the data returned by the URL response.

Examples

create wap my_wap defaults-from wap

Creates a monitor named **my_wap** that inherits properties from the default WAP monitor.

list wap

Displays the properties of all of the WAP monitors.

Options

- **accounting-node**
  Specifies the RADIUS server that provides authentication for the WAP target. Note that if you configure the **accounting-port** option, but you do not configure the this option, the system assumes that the RADIUS server and the WAP server are the same system.
- **accounting-port**
  Specifies the port that the monitor uses for RADIUS accounting. The default value is **none**. A value of **0** (zero) disables RADIUS accounting.
- **app-service**
  Specifies the name of the application service to which the monitor belongs. The default value is **none**. **Note:** If the **strict-updates** option is **enabled** on the application service that owns the object, you cannot modify or delete the monitor. Only the application service can modify or delete the monitor.
- **call-id**
  Specifies the 11-digit phone number for the RADIUS server. The default value is **none**.
- **debug**
  Specifies whether the monitor sends error messages and additional information to a log file created and labeled specifically for this monitor. You can use the log information to help diagnose and troubleshoot unsuccessful health checks. The default value is **no**.
  The options are:
  - **no**
    Specifies that the system does not redirect error messages and additional information related to this monitor.

- **yes**
  Specifies that the system redirects error messages and additional information to the /var/log/monitors/<monitor_name>-<node_name>-<port>.log file.

- **defaults-from**
  Specifies the name of the monitor from which you want your custom monitor to inherit settings. The default value is **wap**.
- **description**
  User defined description.
- **destination**
  Specifies the IP address and service port of the resource that is the destination of this monitor. The default value is ***:***.
  Possible values are:
  - ***:***
    Specifies to perform a health check on the IP address and port supplied by a pool member.
  - ***:port**
    Specifies to perform a health check on the server with the IP address supplied by the pool member and the port you specify.
  - **IP address:port**
    Specifies to mark a pool member **up** or **down** based on the response of the server at the IP address and port you specify.
- **glob**
  Displays the items that match the **glob** expression. See **help glob** for a description of **glob** expression syntax.
- **framed-address**
  Specifies the RADIUS framed IP address. The default value is **none**.
- **interval**
  Specifies, in seconds, the frequency at which the system issues the monitor check when either the resource is **down** or the status of the resource is unknown. The default value is **10** seconds.

Important

*F5 Networks recommends that when you configure this option and the **up-interval** option, whichever value is greater be a multiple of the lesser value to allow for an even distribution of monitor checks among all monitors.*

- **manual-resume**
  Specifies whether the system automatically changes the status of a resource to **up** at the next successful monitor check. The default value of the manual-resume option is **disabled**.
  Note that if you set the **manual-resume** option to **enabled**, you must manually mark the resource as **up** before the system can use it for load balancing connections.

- **name**
  Specifies a unique name for the component. This option is required for the commands **create**, **delete**, and **modify**.
- **partition**
  Displays the administrative partition within which the component resides.
- **recv**
  Specifies the text string that the monitor looks for in the returned resource. The most common receive expressions contain a text string that is included in an HTML file on your site. The text string can be regular text, HTML tags, or image names. If you do not specify both a value for both the **send** and **recv** options, the monitor performs a simple service check and connect only. The default value is **none**.
- **regex**
  Displays the items that match the regular expression. The regular expression must be preceded by an at sign (@[regular expression]) to indicate that the identifier is a regular expression. See **help regex** for a description of regular expression syntax.
- **secret**
  Specifies the password the monitor needs to access the resource. The default value is **none**.
- **send**
  Specifies the text string that the monitor sends to the target object. The default setting is **GET /**, which retrieves a default HTML file for a web site.
  To retrieve a specific page from a web site, specify a fully-qualified path name, for example, **GET /www/company/index.html**. Since the string may have special characters, the system may require that the string be enclosed with single quotation marks.
  If this value is null, then a valid connection suffices to determine that the service is **up**. In this case, the system does not need the **recv** option and ignores the option even if it is not null. The default value is **none**.
- **server-id**
  Specifies the RADIUS NAS-ID for this system when configuring a RADIUS server. The default value is **none**.
- **session-id**
  Specifies the RADIUS session identification number when configuring a RADIUS server. The default value is **none**.
- **time-until-up**
  Specifies the amount of time, in seconds, after the first successful response before a node is marked **up**. A value of **0** (zero) causes a node to be marked **up** immediately after a valid response is received from the node. The default value is **0** (zero).
- **timeout**
  Specifies the number of seconds the target has in which to respond to the monitor request. The default value is **31** seconds.
  If the target responds within the set time period, it is considered **up**. If the target does not respond within the set time period, it is considered **down**.

Also, if the target responds with a RESET packet, the system immediately flags the target as **down** without waiting for the timeout interval to expire.

- **up-interval**
  Specifies, in seconds, the frequency at which the system issues the monitor check when the resource is **up**. The default value is **0** (zero), which specifies that the system uses the value of the **interval** option whether the resource is **up** or **down**.

Important

*F5 Networks recommends that when you configure this option and the **interval** option, whichever value is greater be a multiple of the lesser value to allow for an even distribution of monitor checks among all monitors.*

See Also

create, *delete*, *edit*, glob, *list*, *modify*, regex, *show*, *tmsh*

wmi

Configures a Windows Management Infrastructure (WMI) monitor.

Syntax

Configure the **wmi** component within the **ltm monitor** module using the syntax in the following sections.

Create/Modify

```
create wmi [name]
modify wmi [name]
    agent [string]
    app-service [[string] | none]
    command [ [command] | none ]
    defaults-from [name]
    description [string]
    interval [integer]
    metrics [ [value] | none]
    password [none | [password] ]
    time-until-up [integer]
    timeout [integer]
    url [none | [URL] ]
    username [ [name] | none]
edit wmi [ [ [name] | [glob] | [regex] ] ... ]
    all-properties
    non-default-properties
```

Display

```
list wmi
list wmi [ [ [name] | [glob] | [regex] ] ... ]
show wmi [ [ [name] | [glob] | [regex] ] ... ]
show running-config wmi
show running-config wmi [ [ [name] | [glob] | [regex] ] ... ]
    agent
    all-properties
    method
    non-default-properties
    one-line
    partition
    post
```

Delete

```
delete wmi [name]
```

◆ Note

You cannot delete default monitors.

Description

You can use the **wmi** component to configure a custom monitor, or you can use the default WMI monitor that the Local Traffic Manager provides. This type of monitor checks the performance of a pool, pool member, or virtual server that is running the WMI data collection agent, and then dynamically load balances traffic accordingly.

Examples

create wmi my_wmi defaults-from wmi

Creates a monitor named **my_wmi** that inherits properties from the default WMI monitor.

list wmi

Displays the properties of all of the WMI monitors.

Options

- **agent**
  Displays the agent for the monitor. The default agent is **Mozilla/4.0 (compatible: MSIE 5.0; Windows NT)**.
- **app-service**
  Specifies the name of the application service to which the monitor belongs. The default value is **none**. **Note:** If the **strict-updates** option is **enabled** on the application service that owns the object, you cannot modify or delete the monitor. Only the application service can modify or delete the monitor.
- **command**
  Specifies the command that the system uses to obtain the metrics from the resource. See the documentation for this resource for information on available commands.
- **defaults-from**
  Specifies the name of the monitor from which you want your custom monitor to inherit settings. The default value is **wmi**.
- **description**
  User defined description.
- **glob**
  Displays the items that match the **glob** expression. See **help glob** for a description of **glob** expression syntax.
- **interval**
  Specifies the frequency at which the system issues the monitor check. The default value is **5** seconds.
- **method**
  Displays the GET method. You cannot modify the method.

- **metrics**
  Specifies the performance metrics that the commands collect from the target. The default value is **LoadPercentage, DiskUsage, PhysicalMemoryUsage:1.5, VirtualMemoryUsage:2.0**.
- **name**
  Specifies a unique name for the component. This option is required for the commands **create**, **delete**, and **modify**.
- **partition**
  Displays the administrative partition within which the component resides.
- **password**
  Specifies the password if the monitored target requires authentication. The default value is **none**.
- **post**
  Specifies the mechanism that the monitor uses for posting. The default value is **RespFormat=HTML**.
- **regex**
  Displays the items that match the regular expression. The regular expression must be preceded by an at sign (@[regular expression]) to indicate that the identifier is a regular expression. See **help regex** for a description of regular expression syntax.
- **time-until-up**
  Specifies the amount of time, in seconds, after the first successful response before a node is marked **up**. A value of **0** (zero) causes a node to be marked **up** immediately after a valid response is received from the node. The default value is **0** (zero).
- **timeout**
  Specifies the number of seconds the target has in which to respond to the monitor request. The default value is **16** seconds.
  If the target responds within the set time period, it is considered **up**. If the target does not respond within the set time period, it is considered **down**. Also, if the target responds with a RESET packet, the system immediately flags the target as **down** without waiting for the timeout interval to expire.
- **url**
  Specifies the URL that the monitor uses. The default value is **/scripts/f5Isapi.dll**.
- **username**
  Specifies the user name if the monitored target requires authentication. The default value is **none**.

See Also

create, *delete*, *edit*, glob, *list*, *modify*, regex, *show*, *tmsh*

66

ltm persistence

- Introducing the ltm persistence module
- Alphabetical list of components

Introducing the ltm persistence module

You can use the tmsh components that reside within the ltm persistence module to configure persistence for the BIG-IP® system. For more information about the tmsh hierarchical structure, see Chapter 2, *Understanding and Using the Traffic Management Shell*.

Alphabetical list of components

The remainder of this chapter lists the tmsh components that are available in the ltm persistence module.

cookie

Configures a cookie persistence profile.

Syntax

Configure the **cookie** component within the **ltm persistence** module using the syntax in the following sections.

Modify

```
create cookie [name]
modify cookie [name]
    all
    always-send [enabled | disabled]
    app-service [[string] | none]
    cookie-name [ [name] | none]
    cookie-encryption [required | preferred | disabled]
    cookie-encryption-passphrase [string | none]
    defaults-from [name]
    description [string]
    expiration [ [d:h:m:s] | [h:m:s] | [m:s] | [seconds]
                | "session cookie"]
    hash-length [integer]
    hash-offset [integer]
    match-across-pools [enabled | disabled]
    match-across-services [enabled | disabled]
    match-across-virtuals [enabled | disabled]
    method [hash | insert | passive | rewrite]
    mirror [enabled | disabled]
    override-connection-limit [enabled | disabled]
    timeout [indefinite | [integer] ]
edit cookie [ [ [name] | [glob] | [regex] ] ... ]
    all-properties
    non-default-properties
mv cookie [ [[source-name] [destination-name]] | [[name] to-folder [folder-name]] |
[[name...name] to-folder [folder-name]] ]
    to-folder
```

Display

```
list cookie
list cookie [ [ [name] | [glob] | [regex] ] ... ]
show running-config cookie
show running-config cookie [ [ [name] | [glob] | [regex] ] ... ]
    all
    all-properties
    non-default-properties
    one-line
    partition
```

Delete

```
delete cookie [name]
    all
```

Description

You can use the **cookie** component to configure cookie persistence for the BIG-IP® system. Cookie persistence uses an HTTP cookie stored on a client's computer to allow the client to connect to the same server previously visited at a web site.

A persistence profile is a profile that enables persistence when you assign the profile to a virtual server. Using a persistence profile avoids having to write an iRule to implement a type of persistence. You can either use the default profile, or create a custom profile based on the default.

Examples

list cookie

Displays all cookie persistence profiles.

create cookie cookie_persistence defaults-from cookie

Creates a custom cookie persistence profile named **cookie_persistence** that inherits its settings from the default cookie persistence profile.

mv cookie /Common/my_cookie_profile to-folder /Common/my_folder

Moves a custom cookie persistence profile named **my_cookie_profile** to a folder named **my_folder**, where **my_folder** has already been created and exists within **/Common**.

Options

- **always-send**
  Send the cookie persistence entry on every reply, even if the entry has previously been supplied to the client. The default value is **disabled**.
- **app-service**
  Specifies the name of the application service to which the profile belongs. The default value is **none**. **Note:** If the **strict-updates** option is **enabled** on the application service that owns the object, you cannot modify or delete the profile. Only the application service can modify or delete the profile.
- **cookie-name**
  Specifies a unique name for the cookie. This option is required.
- **defaults-from**
  Specifies the existing profile from which the system imports settings for the new profile. The default value is **cookie**, the system default cookie persistence profile.
- **description**
  User defined description.

- **cookie-encryption**
  Specifies the way in which cookie format will be used: disabled: generate old format,unencrypted, preferred: generate encrypted cookie but accept both encrypted and old format, and required: cookie format must be encrypted. Default is required.
- **cookie-encryption-passphrase**
  Specifies a passphrase to be used for cookie encryption.
- **expiration**
  Specifies the cookie expiration date in the format d:h:m:s, h:m:s, m:s or seconds. (hours 0-23, minutes 0-59, seconds 0-59). The time period must be less than 24856 days.
  You can use **"session-cookie"** (0 seconds) to indicate that the cookie expires when the browser closes.
- **glob**
  Displays the items that match the **glob** expression. See **help glob** for a description of **glob** expression syntax.
- **hash-length**
  Specifies the cookie hash length. The length is the number of bytes to use when calculating the hash value. The default value is **0** (zero) bytes.
- **hash-offset**
  Specifies the cookie hash offset. The offset is the number of bytes in the cookie to skip before calculating the hash value. The default value is **0** (zero) bytes.
- **match-across-pools**
  Specifies, when **enabled**, that the system can use any pool that contains this persistence record. The default value is **disabled**.
- **match-across-services**
  Specifies, when **enabled**, that all persistent connections from a client IP address, which go to the same virtual IP address, also go to the same node. The default value is **disabled**.
- **match-across-virtuals**
  Specifies, when **enabled**, that all persistent connections from the same client IP address go to the same node. The default value is **disabled**.
- **method**
  Specifies the type of cookie processing that the system uses. The default value is **insert**.
- **mirror**
  Specifies whether the system mirrors persistence records to the high-availability peer. This option is applicable only when the value of the **method** option is **hash**. The default value is **disabled**.
- **name**
  Specifies a unique name for the component. This option is required for the commands **create**, **delete**, and **modify**.
- **override-connection-limit**
  Specifies, when **enabled**, that the pool member connection limits are not enforced for persisted clients. Per-virtual connection limits remain hard limits and are not disabled. The default value is **disabled**.

- **partition**
  Displays the administrative partition within which the component resides.
- **regex**
  Displays the items that match the regular expression. The regular expression must be preceded by an at sign (@[regular expression]) to indicate that the identifier is a regular expression. See **help regex** for a description of regular expression syntax.
- **timeout**
  Specifies the duration of the persistence entries. The default value is **0** (zero) seconds.
- **to-folder**
  cookie persistence profiles can be moved to any folder under **/Common**, but configuration dependencies may restrict moving the profile out of **/Common**.

See Also

create, *delete*, *edit*, glob, *list*, *virtual*, *modify*, *mv*, regex, *show*, *tmsh*

dest-addr

Configures a destination address affinity persistence profile.

Syntax

Configure the **dest-addr** component within the **ltm persistence** module using the syntax in the following sections.

Modify

```
create dest-addr [name]
modify dest-addr [name]
    all
    app-service [[string] | none]
    defaults-from [name]
    description [string]
    hash-algorithm [carp | default]
    mask [ [ip address] | none]
    match-across-pools [ enabled | disabled]
    match-across-services [enabled | disabled]
    match-across-virtuals [enabled | disabled]
    mirror [enabled | disabled]
    override-connection-limit [enabled | disabled]
    timeout [integer]
edit dest-addr [ [ [name] | [glob] | [regex] ] ... ]
    all-properties
    non-default-properties
mv dest-addr [ [[source-name] [destination-name]] | [[name] to-folder [folder-name]] |
[[name...name] to-folder [folder-name]] ]
    to-folder
```

Display

```
list dest-addr
list dest-addr [ [ [name] | [glob] | [regex] ] ... ]
show running-config dest-addr
show running-config dest-addr [ [ [name] | [glob] | [regex] ] ... ]
    all
    all-properties
    non-default-properties
    one-line
    partition
```

Delete

```
delete dest-addr [name]
    all
```

Description

You can use the **dest-addr** component to configure a destination address affinity persistence profile for the BIG-IP® system. Also known as sticky persistence, destination address affinity persistence supports TCP and UDP protocols, and directs session requests to the same server based solely on the destination IP address of a packet.

A persistence profile is a profile that enables persistence when you assign the profile to a virtual server. Using a persistence profile means that you do not have to write an iRule to implement a type of persistence. You can either use the default profile, or create a custom profile based on the default.

Examples

list dest-addr

Displays all destination address affinity persistence profiles.

create dest-addr da_persistence defaults-from dest-addr

Creates a custom destination address affinity persistence profile named **da_persistence** that inherits its settings from the default destination address affinity persistence profile.

mv dest-addr /Common/my_dest-addr_profile to-folder /Common/my_folder

Moves a custom destination address persistence profile named **my_dest-addr_profile** to a folder named **my_folder**, where **my_folder** has already been created and exists within **/Common**.

Options

- **app-service**
  Specifies the name of the application service to which the profile belongs. The default value is **none**. **Note:** If the **strict-updates** option is **enabled** on the application service that owns the object, you cannot modify or delete the profile. Only the application service can modify or delete the profile.
- **defaults-from**
  Specifies the existing profile from which the system imports settings for the new profile. The default value is **dest_addr**, the system default destination address affinity persistence profile.
- **description**
  User defined description.
- **glob**
  Displays the items that match the **glob** expression. See **help glob** for a description of **glob** expression syntax.

- **hash-algorithm**
  Specifies the system uses hash persistence load balancing. The default value is default (no hash persistence).
  The options are:
  - **carp**
    Specifies to use the Cache Array Routing Protocol (CARP) to select the pool member for LB. The input to CARP is the hash value of destination address.
  - **default**
    no hash persistence.
- **mask**
  Specifies an IP mask. This is the mask used by simple persistence for connections. The default value is **::**.
- **match-across-pools**
  Specifies, when **enabled**, that the system can use any pool that contains this persistence record. The default value is **disabled**.
- **match-across-services**
  Specifies, when **enabled**, that all persistent connections from a client IP address, which go to the same virtual IP address, also go to the same node. The default value is **disabled**.
- **match-across-virtuals**
  Specifies, when **enabled**, that all persistent connections from the same client IP address go to the same node. The default value is **disabled**.
- **mirror**
  Specifies whether the system mirrors persistence records to the high-availability peer. The default value is **disabled**.
- **name**
  Specifies a unique name for the component. This option is required for the commands **create**, **delete**, and **modify**.
- **override-connection-limit**
  Specifies, when **enabled**, that the pool member connection limits are not enforced for persisted clients. Per-virtual connection limits remain hard limits and are not disabled. The default value is **disabled**.
- **partition**
  Displays the administrative partition within which the component resides.
- **regex**
  Displays the items that match the regular expression. The regular expression must be preceded by an at sign (@[regular expression]) to indicate that the identifier is a regular expression. See **help regex** for a description of regular expression syntax.
- **timeout**
  Specifies the duration of the persistence entries. The default value is **180** seconds.

- **to-folder**
  dest-addr persistence profiles can be moved to any folder under **/Common**, but configuration dependencies may restrict moving the profile out of **/Common**.

See Also

create, *delete*, *edit*, glob, *list*, *virtual*, *modify*, *mv*, regex, *show*, *tmsh*

global-settings

Configures persistence for the BIG-IP® system.

Syntax

Configure the **global-settings** component within the **ltm persistence** module using the syntax in the following sections.

Modify

```
modify global-settings [option name]
    description [string]
    dest-addr-limit-mode [timeout | maxcount]
    dest-addr-max [integer]
    proxy-group [string]

edit global-settings [ [ [name] | [glob] | [regex] ] ... ]
    all-properties
    non-default-properties
```

Display

```
list global-settings
list global-settings [ [ [name] | [glob] | [regex] ] ... ]
show running-config global-settings
show running-config global-settings
                    [ [ [name] | [glob] | [regex] ] ... ]
    all-properties
    non-default-properties
    one-line
```

Description

You can use the **global-settings** component within the **ltm persistence** module to configure persistence for the system.

For information about configuring session persistence for a virtual server, see the man pages for the following components: **ltm persistence hash**, **ltm persistence msrdp**, **ltm persistence sip**, **ltm persistence source-addr**, **ltm persistence ssl**, and **ltm persistence universal**.

Examples

list global-settings

Displays the global persistence configuration.

modify global-settings dest-addr-limit-mode maxcount

Sets the value of the option **dest-addr-limit-mode** to **maxcount**, which indicates that a persistence session is limited by the maximum number of requests to the destination address.

Options

- **description**
  User defined description.
- **dest-addr-limit-mode**
  Specifies that a persistence session is limited by either the number of seconds before the persistence entry times out, or by a maximum number of requests to the destination address. The default value is **timeout**.
- **dest-addr-max**
  Specifies the maximum number of entries that the persistence table can contain at any one time, when the value of the option **dest-addr-limit-mode** is **maxcount**. The default value is **2048** entries.
- **glob**
  Displays the items that match the **glob** expression. See **help glob** for a description of **glob** expression syntax.
- **proxy-group**
  Specifies a group of servers that are configured to process all of the requests from a single source address during a persistence session. The default value is **aol**.
- **regex**
  Displays the items that match the regular expression. The regular expression must be preceded by an at sign (@[regular expression]) to indicate that the identifier is a regular expression. See **help regex** for a description of regular expression syntax.

See Also

list, *virtual*, *modify*, regex, *show*, *tmsh*

hash

Configures a hash persistence profile.

Syntax

Configure the **hash** component within the **ltm persistence** module using the syntax in the following sections.

Modify

```
create hash [name]
modify hash [name]
    all
    app-service [[string] | none]
    defaults-from [name]
    description [string]
    hash-algorithm [carp | default]
    hash-buffer-limit [integer]
    hash-end-pattern [none | [string] ]
    hash-length [integer]
    hash-offset [integer]
    hash-start-pattern [none | [string] ]
    match-across-pools [enabled | disabled]
    match-across-services [enabled | disabled]
    match-across-virtuals [enabled | disabled]
    mirror [enabled | disabled]
    override-connection-limit [enabled | disabled]
    rule [iRule name]
    timeout [integer]
edit hash [ [ [name] | [glob] | [regex] ] ... ]
    all-properties
    non-default-properties
mv hash [ [[source-name] [destination-name]] | [[name] to-folder [folder-name]] |
[[name...name] to-folder [folder-name]] ]
    to-folder
```

Display

```
list hash
list hash [ [ [name] | [glob] | [regex] ] ... ]
show running-config hash
show running-config hash [ [ [name] | [glob] | [regex] ] ... ]
    all
    all-properties
    non-default-properties
    one-line
    partition
```

Delete

```
delete hash [name]
    all
```

Description

You can use the **hash** component to configure a hash persistence profile for the BIG-IP® system. Hash persistence can also be activated from an existing iRule.

A persistence profile is a profile that enables persistence when you assign the profile to a virtual server. Using a persistence profile means that you do not have to write an iRule to implement a type of persistence. You can either use the default profile, or create a custom profile based on the default.

Examples

list hash

Displays all hash persistence profiles.

create hash hash_persistence defaults-from hash

Creates a custom hash persistence profile named **hash_persistence** that inherits its settings from the default hash persistence profile.

mv hash /Common/my_hash_profile to-folder /Common/my_folder

Moves a custom hash persistence profile named **my_hash_profile** to a folder named **my_folder**, where **my_folder** has already been created and exists within **/Common**.

Options

- **app-service**
  Specifies the name of the application service to which the profile belongs. The default value is **none**. **Note:** If the **strict-updates** option is **enabled** on the application service that owns the object, you cannot modify or delete the profile. Only the application service can modify or delete the profile.
- **defaults-from**
  Specifies the existing profile from which the system imports settings for the new profile. The default value is **hash**, the system default cookie persistence profile.
- **description**
  User defined description.
- **glob**
  Displays the items that match the **glob** expression. See **help glob** for a description of **glob** expression syntax.
- **hash-algorithm**
  Specifies the algorithm the system uses for hash persistence load balancing. The default value is default.
  The options are:

- **carp**
  Specifies to use the Cache Array Routing Protocol (CARP) to select the pool member for LB.
- **default**
  Specifies to use indexing of pool members to select the pool member for LB.

◆ **hash-buffer-limit**
Specifies the maximum buffer length the system collects to locate the hashing pattern for hash persistence load balancing. The default value is **0** (zero).

◆ **hash-end-pattern**
Specifies the string that describes the ending location of the hash pattern that the system uses to perform hash persistence load balancing. The default value is **none**.

◆ **hash-length**
Specifies the length of data within the packet in bytes that the system uses to calculate the hash value when performing hash persistence load balancing. The default value is **0** (zero) bytes.

◆ **hash-offset**
Specifies the start offset within the packet from which the system begins the hash when performing hash persistence load balancing. The default value is **0** (zero).

◆ **hash-start-pattern**
Specifies the string that describes the start location of the hash pattern that the system uses to perform hash persistence load balancing. The default value is **none**.

◆ **match-across-pools**
Specifies, when **enabled**, that the system can use any pool that contains this persistence record. The default value is **disabled**.

◆ **match-across-services**
Specifies, when **enabled**, that all persistent connections from a client IP address, which go to the same virtual IP address, also go to the same node. The default value is **disabled**.

◆ **match-across-virtuals**
Specifies, when **enabled**, that all persistent connections from the same client IP address go to the same node. The default value is **disabled**.

◆ **mirror**
Specifies whether the system mirrors persistence records to the high-availability peer. The default value is **disabled**.

◆ **name**
Specifies a unique name for the component. This option is required for the commands **create**, **delete**, and **modify**.

◆ **override-connection-limit**
Specifies, when **enabled**, that the pool member connection limits are not enforced for persisted clients. Per-virtual connection limits remain hard limits and are not disabled. The default value is **disabled**.

- **partition**
  Displays the administrative partition within which the component resides.
- **regex**
  Displays the items that match the regular expression. The regular expression must be preceded by an at sign (@[regular expression]) to indicate that the identifier is a regular expression. See **help regex** for a description of regular expression syntax.
- **rule**
  Specifies a rule name, if you are using a rule for universal persistence.
- **timeout**
  Specifies the duration of the persistence entries. The default value is **180** seconds.
- **to-folder**
  hash persistence profiles can be moved to any folder under **/Common**, but configuration dependencies may restrict moving the profile out of **/Common**.

See Also

create, *delete*, *edit*, glob, *list*, *virtual*, *modify*, *mv*, regex, *show*, *tmsh*

msrdp

Configures a Microsoft® Remote Display Protocol (MSRDP) persistence profile.

Syntax

Configure the **msrdp** component within the **ltm persistence** module using the syntax in the following sections.

Modify

```
create msrdp [name]
modify msrdp [name]
    all
    app-service [[string] | none]
    defaults-from [name]
    description [string]
    has-session-dir [no | yes]
    match-across-pools [enabled | disabled]
    match-across-services [enabled | disabled]
    match-across-virtuals [enabled | disabled]
    mirror [enabled | disabled]
    override-connection-limit [enabled | disabled]
    timeout [integer]
edit msrdp [ [ [name] | [glob] | [regex] ] ... ]
    all-properties
    non-default-properties
mv msrdp [ [[source-name] [destination-name]] | [[name] to-folder [folder-name]] |
[[name...name] to-folder [folder-name]] ]
    to-folder
```

Display

```
list msrdp
list msrdp [ [ [name] | [glob] | [regex] ] ... ]
show running-config msrdp
show running-config msrdp [ [ [name] | [glob] | [regex] ] ... ]
    all
    all-properties
    non-default-properties
    one-line
    partition
```

Delete

```
delete msrdp [name]
    all
```

Description

You can use the **msrdp** component to configure an MSRDP persistence profile for the BIG-IP® system. MSRDP persistence provides an efficient way of load balancing traffic and maintaining persistent sessions between Windows clients and servers that are running the Microsoft Terminal Services service. The recommended scenario for enabling the MSRDP persistence feature is to create a load balancing pool that consists of members running Windows .NET Server 2003, Enterprise Edition, or later, where all members belong to a Windows cluster and participate in a Windows session directory.

A persistence profile is a profile that enables persistence when you assign the profile to a virtual server. Using a persistence profile means that you do not have write an iRule to implement a type of persistence. You can either use the default profile, or create a custom profile based on the default.

Examples

list msrdp

Displays all MSRDP persistence profiles.

create msrdp msrdp_persistence defaults-from msrdp

Creates a custom MSRDP persistence profile named **msrdp_persistence** that inherits its settings from the default MSRDP persistence profile

mv msrdp /Common/my_msrdp_profile to-folder /Common/my_folder

Moves a custom MSRDP persistence profile named **my_msrdp_profile** to a folder named **my_folder**, where **my_folder** has already been created and exists within **/Common**.

Options

- **app-service**
  Specifies the name of the application service to which the profile belongs. The default value is **none**. **Note:** If the **strict-updates** option is **enabled** on the application service that owns the object, you cannot modify or delete the profile. Only the application service can modify or delete the profile.
- **defaults-from**
  Specifies the existing profile from which the system imports settings for the new profile. The default value is **msrdp**, the system default cookie persistence profile.
- **description**
  User defined description.
- **glob**
  Displays the items that match the **glob** expression. See **help glob** for a description of **glob** expression syntax.

- **has-session-dir**
  Specifies whether the Microsoft terminal services are configured with a session directory, so the system does not load balance the initial connection. The default value is **yes**.
- **match-across-pools**
  Specifies, when **enabled**, that the system can use any pool that contains this persistence record. The default value is **disabled**.
- **match-across-services**
  Specifies, when **enabled**, that all persistent connections from a client IP address, which go to the same virtual IP address, also go to the same node. The default value is **disabled**.
- **match-across-virtuals**
  Specifies, when **enabled**, that all persistent connections from the same client IP address go to the same node. The default value is **disabled**.
- **mirror**
  Specifies whether the system mirrors persistence records to the high-availability peer. The default value is **disabled**.
- **name**
  Specifies a unique name for the component. This option is required for the commands **create**, **delete**, and **modify**.
- **override-connection-limit**
  Specifies, when **enabled**, that the pool member connection limits are not enforced for persisted clients. Per-virtual connection limits remain hard limits and are not disabled. The default value is **disabled**.
- **partition**
  Displays the administrative partition within which the component resides.
- **regex**
  Displays the items that match the regular expression. The regular expression must be preceded by an at sign (@[regular expression]) to indicate that the identifier is a regular expression. See **help regex** for a description of regular expression syntax.
- **timeout**
  Specifies the duration of the persistence entries. The default value is **300** seconds.
- **to-folder**
  msrdp persistence profiles can be moved to any folder under **/Common**, but configuration dependencies may restrict moving the profile out of **/Common**.

See Also

create, *delete*, *edit*, glob, *list*, *virtual*, *modify*, *mv*, regex, *show*, *tmsh*

persist-records

Displays or deletes persistence records.

Syntax

Configure the **persist-records** component within the **ltm persistence** module using the syntax in the following sections.

Display

```
show persist-records
    client-addr [ip address]
    key [string]
    mode [cookie | destination-address | hash | msrdp | sip |
      source-address | ssl-session-id | universal]
    node-addr [ip address]
    node-port [integer]
    pool [string]
    save-to-file [ filename ]
    virtual [string]
```

Delete

```
delete persist-records
    client-addr [ip address]
    key [string]
    mode [cookie | destination-address | hash | msrdp | sip |
      source-address | ssl-session-id | universal]
    node-addr [ip address]
    node-port [integer]
    pool [string]
    virtual [string]
```

Description

You can use the **persist-records** component to either display or delete records of persistent connections.

Examples

show persist-records

Displays all persistent connections on the BIG-IP® system.

delete persist-records client-addr 172.19.255.1

Deletes all persistent connections that originate from the client IP address, **172.19.255.1**.

Options

- **client-addr**
  Specifies the IP address of the client from which the persistent connections you want to view or delete persist.
- **key**
  Specifies a string that the system is using to persist the connections you want to view or delete.
- **mode**
  Specifies the type of persistence of the connections you want to view or delete. The options are:
  - **cookie**
    Cookie persistence uses an HTTP cookie stored on a client's computer to allow the client to connect to the same server previously visited at a web site.
  - **destination-address**
    Also known as sticky persistence, destination address affinity persistence supports TCP and UDP protocols, and directs session requests to the same server based solely on the destination IP address of a packet.
  - **hash**
    Hash persistence is based on an existing iRule.
  - **msrdp**
    MSRDP persistence provides an efficient way of load balancing traffic and maintaining persistent sessions between Windows® clients and servers that are running the Microsoft® Terminal Services service. The recommended scenario for enabling the MSRDP persistence feature is to create a load balancing pool that consists of members running Windows .NET Server 2003, Enterprise Edition, or later, where all members belong to a Windows cluster and participate in a Windows session directory.
  - **sip**
    Session Initiation Protocol (SIP) persistence is a type of persistence available for server pools. You can configure SIP persistence for proxy servers that receive SIP messages sent through UDP. The BIG-IP system currently supports persistence for SIP messages sent through UDP, TCP, or SCTP.
  - **source-address**
    Also known as simple persistence, source address affinity persistence supports TCP and UDP protocols, and directs session requests to the same server based solely on the source IP address of a packet. When you specify a source address as the mode of persistence, you must specify an IP address using the **client-addr** option.
  - **ssl-session-id**
    SSL persistence is a type of persistence that tracks non-terminated SSL sessions, using the SSL session ID. Even when the client's IP address changes, the system still recognizes the connection as being persistent based on the session ID. Note that the term, non-terminated

SSL sessions, refers to sessions in which the system does not perform the tasks of SSL certificate authentication and encryption/re-encryption.

- **universal**
  Universal persistence allows you to write an expression that defines what to persist on in a packet. The expression, written using the same expression syntax that you use in iRules®, defines some sequence of bytes to use as a session identifier.

- **node-addr**
  Specifies the IP address of the node with which the client sessions that you want to view or delete remain persistent.
- **node-port**
  Specifies the port number of the node with which the client sessions that you want to view or delete remain persistent.
- **pool**
  Specifies the pool member with which the client sessions that you want to view or delete remain persistent.
- **save-to-file**
  Specifies the file which persist-records information can be save to. With this option, it can write a file larger than 2GB.
- **virtual**
  Specifies the virtual server with which the client sessions that you want to view or delete remain persistent.

See Also

delete, *show*, *tmsh*

sip

Configures a Session Initiation Protocol (SIP) persistence profile.

Syntax

Configure the **sip** component within the **ltm persistence** module using the syntax in the following sections.

Modify

```
create sip [name]
modify sip [name]
    all
    app-service [[string] | none]
    defaults-from [name]
    description [string]
    match-across-pools [ enabled | disabled]
    match-across-services [enabled | disabled]
    match-across-virtuals [enabled | disabled]
    mirror [enabled | disabled]
    override-connection-limit [enabled | disabled]
    sip-info [Call-ID | From | none | SIP-ETag | Subject | To]
    timeout [integer]
edit sip [ [ [name] | [glob] | [regex] ] ... ]
    all-properties
    non-default-properties
mv sip [ [[source-name] [destination-name]] | [[name] to-folder [folder-name]] |
[[name...name] to-folder [folder-name]] ]
    to-folder
```

Display

```
list sip
list sip [ [ [name] | [glob] | [regex] ] ... ]
show running-config sip
show running-config sip [ [ [name] | [glob] | [regex] ] ... ]
    all
    all-properties
    non-default-properties
    one-line
    partition
```

Delete

```
delete sip [name]
    all
```

Description

You can use the **sip** component to configure a SIP persistence profile for the BIG-IP® system. SIP persistence is a type of persistence available for server pools. You can configure SIP persistence for proxy servers that receive SIP messages sent through UDP. The BIG-IP system currently supports persistence for SIP messages sent through UDP, TCP, or SCTP.

A persistence profile is a profile that enables persistence when you assign the profile to a virtual server. Using a persistence profile means that you do not have write an iRule to implement a type of persistence. You can either use the default profile, or create a custom profile based on the default.

Examples

list sip

Displays all SIP persistence profiles.

create sip sip_persistence defaults-from sip_info

Creates a custom SIP persistence profile named **sip_persistence** that inherits its settings from the default SIP persistence profile.

mv sip /Common/my_sip_profile to-folder /Common/my_folder

Moves a custom SIP persistence profile named **my_sip_profile** to a folder named **my_folder**, where **my_folder** has already been created and exists within **/Common**.

Options

- **app-service**
  Specifies the name of the application service to which the profile belongs. The default value is **none**. **Note:** If the **strict-updates** option is **enabled** on the application service that owns the object, you cannot modify or delete the profile. Only the application service can modify or delete the profile.
- **defaults-from**
  Specifies the existing profile from which the system imports settings for the new profile. The default value is **sip_info**, the system default cookie persistence profile.
- **description**
  User defined description.
- **glob**
  Displays the items that match the **glob** expression. See **help glob** for a description of **glob** expression syntax.
- **match-across-pools**
  Specifies, when **enabled**, that the system can use any pool that contains this persistence record. The default value is **disabled**.

- **match-across-services**
  Specifies, when **enabled**, that all persistent connections from a client IP address, which go to the same virtual IP address, also go to the same node. The default value is **disabled**.
- **match-across-virtuals**
  Specifies, when **enabled**, that all persistent connections from the same client IP address go to the same node. The default value is **disabled**.
- **mirror**
  Specifies whether the system mirrors persistence records to the high-availability peer. The default value is **disabled**.
- **name**
  Specifies a unique name for the component. This option is required for the commands **create**, **delete**, and **modify**.
- **override-connection-limit**
  Specifies, when **enabled**, that the pool member connection limits are not enforced for persisted clients. Per-virtual connection limits remain hard limits and are not disabled. The default value is **disabled**.
- **partition**
  Displays the administrative partition within which the component resides.
- **regex**
  Displays the items that match the regular expression. The regular expression must be preceded by an at sign (@[regular expression]) to indicate that the identifier is a regular expression. See **help regex** for a description of regular expression syntax.
- **sip-info**
  Specifies the SIP header field on which you want SIP sessions to persist. The default value is **none**.
- **timeout**
  Specifies the duration of the persistence entries. The default value is **180** seconds.
- **to-folder**
  sip persistence profiles can be moved to any folder under **/Common**, but configuration dependencies may restrict moving the profile out of **/Common**.

See Also

create, *delete*, *edit*, glob, *list*, *virtual*, *modify*, *mv*, regex, *show*, *tmsh*

source-addr

Configures a source address affinity persistence profile.

Syntax

Configure the **source-addr** component within the **ltm persistence** module using the syntax in the following sections.

Modify

```
create source-addr [name]
modify source-addr [name]
    all
    app-service [[string] | none]
    defaults-from [name]
    description [string]
    map-proxies [enabled | disabled]
    map-proxy-address [ip address]
    map-proxy-class [class name]
    hash-algorithm [carp | default]
    mask [ [ip address] | none]
    match-across-pools [enabled | disabled]
    match-across-services [enabled | disabled]
    match-across-virtuals [enabled | disabled]
    mirror [enabled | disabled]
    override-connection-limit [enabled | disabled]
    timeout [integer]
edit source-addr [ [ [name] | [glob] | [regex] ] ... ]
    all-properties
    non-default-properties
mv source-addr [ [[source-name] [destination-name]] | [[name] to-folder [folder-name]]
| [[name...name] to-folder [folder-name]] ]
    to-folder
```

Display

```
list source-addr
list source-addr[ [ [name] | [glob] | [regex] ] ... ]
show running-config source-addr
show running-config source-addr[ [ [name] | [glob] | [regex] ] ... ]
    all
    all-properties
    non-default-properties
    one-line
    partition
```

Delete

```
delete source-addr [name]
    all
```

Description

You can use the **source-addr** component to configure a source address affinity persistence profile for the BIG-IP® system. Also known as simple persistence, source address affinity persistence supports TCP and UDP protocols, and directs session requests to the same server based solely on the source IP address of a packet.

A persistence profile is a profile that enables persistence when you assign the profile to a virtual server. Using a persistence profile means that you do not have to write an iRule to implement a type of persistence. You can either use the default profile, or create a custom profile based on the default.

Examples

list source-addr

Displays all source address affinity persistence profiles.

create source-addr simple_persistence defaults-from source_addr

Creates a custom source address affinity persistence profile named **simple_persistence** that inherits its settings from the default source address affinity persistence profile.

mv source-addr /Common/my_source-addr_profile to-folder /Common/my_folder

Moves a custom source address persistence profile named **my_source-addr_profile** to a folder named **my_folder**, where **my_folder** has already been created and exists within **/Common**.

Options

- **app-service**
  Specifies the name of the application service to which the profile belongs. The default value is **none**. **Note:** If the **strict-updates** option is **enabled** on the application service that owns the object, you cannot modify or delete the profile. Only the application service can modify or delete the profile.
- **defaults-from**
  Specifies the existing profile from which the system imports settings for the new profile. The default value is **source_addr**, the system default cookie persistence profile.
- **description**
  User defined description.
- **glob**
  Displays the items that match the **glob** expression. See **help glob** for a description of **glob** expression syntax.

- **hash-algorithm**
  Specifies the system uses hash persistence load balancing. The default value is default (no hash persistence).
  The options are:
  - **carp**
    Specifies to use the Cache Array Routing Protocol (CARP) to select the pool member for LB. The input to CARP is the hash value of source address.
  - **default**
    no hash persistence.
- **map-proxies**
  Enables or disables the map proxies attribute. The default value is **disabled**.
  This attribute controls whether a source address will first be checked against an IP data-group/class to determine whether it is a well-known proxy address. If it matches the IP class, then the source address will be mapped to a single IP address for the purposes of persistence. The default well known proxy class is based on a pre-defined data-group "aol" which represents the AOL® company's previously-published list of proxies. Using this feature enables you to use client/source IP address persistence with a simple persist mask, but forces all clients matching the IP class to persist to the same server. The IP data-group/class may also be changed using either the map-proxy-class profile attribute or globally by changing the DB variable Persist.WellKnownProxyClass. Also, the IP address used for mapping a single source IP address for persistence may also be specifically set using the map-proxy-address profile attribute.
- **map-proxy-address**
  Specifies the single IP address to use when the source address matches the proxy data-group/class. The default value is **any** which results in the default behavior of using one of the IP addresses from the proxy data-group/class. Note: This mapped IP address does not have to be contained in the IP data-group/class. It may actually be any IP address since it is only used for keying the persistence record.
- **map-proxy-class**
  Specifies the data-group/class to use for determining whether a source address is from a proxy. The default value is **none** which will result in map_proxies using the class defined by the DB variable Persist.WellKnownProxyClass.
- **mask**
  Specifies an IP mask. This is the mask used by simple persistence for connections. The default value is **::**.
- **match-across-pools**
  Specifies, when **enabled**, that the system can use any pool that contains this persistence record. The default value is **disabled**.
- **match-across-services**
  Specifies, when **enabled**, that all persistent connections from a client IP address, which go to the same virtual IP address, also go to the same node. The default value is **disabled**.

- **match-across-virtuals**
  Specifies, when **enabled**, that all persistent connections from the same client IP address go to the same node. The default value is **disabled**.
- **mirror**
  Specifies whether the system mirrors persistence records to the high-availability peer. The default value is **disabled**.
- **name**
  Specifies a unique name for the component. This option is required for the commands **create**, **delete**, and **modify**.
- **override-connection-limit**
  Specifies, when **enabled**, that the pool member connection limits are not enforced for persisted clients. Per-virtual connection limits remain hard limits and are not disabled. The default value is **disabled**.
- **partition**
  Displays the administrative partition within which the component resides.
- **regex**
  Displays the items that match the regular expression. The regular expression must be preceded by an at sign (@[regular expression]) to indicate that the identifier is a regular expression. See **help regex** for a description of regular expression syntax.
- **timeout**
  Specifies the duration of the persistence entries. The default value is **180** seconds.
- **to-folder**
  source-addr persistence profiles can be moved to any folder under **/Common**, but configuration dependencies may restrict moving the profile out of **/Common**.

See Also

create, *delete*, *edit*, glob, *list*, *virtual*, *modify*, *mv*, regex, *show*, *tmsh*

ssl

Configures a Secure Socket Layer (SSL) persistence profile.

Syntax

Configure the **ssl** component within the **ltm persistence** module using the syntax in the following sections.

Modify

```
create ssl [name]
modify ssl [name]
    all
    app-service [[string] | none]
    defaults-from [name]
    description [string]
    match-across-pools [ enabled | disabled]
    match-across-services [enabled | disabled]
    match-across-virtuals [enabled | disabled]
    mirror [enabled | disabled]
    override-connection-limit [enabled | disabled]
    timeout [integer]
edit ssl [ [ [name] | [glob] | [regex] ] ... ]
   all-properties
   non-default-properties
mv ssl [ [[source-name] [destination-name]] | [[name] to-folder [folder-name]] |
[[name...name] to-folder [folder-name]] ]
    to-folder
```

Display

```
list ssl
list ssl [ [ [name] | [glob] | [regex] ] ... ]
show running-config ssl
show running-config ssl [ [ [name] | [glob] | [regex] ] ... ]
    all
    all-properties
    non-default-properties
    one-line
    partition
```

Delete

```
delete ssl [name]
    all
```

Description

You can use the **ssl** component to configure a destination address affinity persistence profile for the BIG-IP® system. SSL persistence is a type of persistence that tracks non-terminated SSL sessions, using the SSL session

ID. Even when the client's IP address changes, the system still recognizes the connection as being persistent based on the session ID. Note that the term, non-terminated SSL sessions, refers to sessions in which the system does not perform the tasks of SSL certificate authentication and encryption/re-encryption.

A persistence profile is a profile that enables persistence when you assign the profile to a virtual server. Using a persistence profile means that you do not have to write an iRule to implement a type of persistence. You can either use the default profile, or create a custom profile based on the default.

Examples

list ssl

Displays all SSL persistence profiles.

create ssl ssl_persistence defaults-from ssl

Creates a custom SSL persistence profile named **ssl_persistence** that inherits its settings from the default SSL persistence profile.

mv ssl /Common/my_ssl_profile to-folder /Common/my_folder

Moves a custom SSL persistence profile named **my_ssl_profile** to a folder named **my_folder**, where **my_folder** has already been created and exists within **/Common**.

Options

- **app-service**
  Specifies the name of the application service to which the profile belongs. The default value is **none**. **Note:** If the **strict-updates** option is **enabled** on the application service that owns the object, you cannot modify or delete the profile. Only the application service can modify or delete the profile.
- **defaults-from**
  Specifies the existing profile from which the system imports settings for the new profile. The default value is **ssl**, the system default cookie persistence profile.
- **description**
  User defined description.
- **glob**
  Displays the items that match the **glob** expression. See **help glob** for a description of **glob** expression syntax.
- **match-across-pools**
  Specifies, when **enabled**, that the system can use any pool that contains this persistence record. The default value is **disabled**.

- **match-across-services**
  Specifies, when **enabled**, that all persistent connections from a client IP address, which go to the same virtual IP address, also go to the same node. The default value is **disabled**.
- **match-across-virtuals**
  Specifies, when **enabled**, that all persistent connections from the same client IP address go to the same node. The default value is **disabled**.
- **mirror**
  Specifies whether the system mirrors persistence records to the high-availability peer. The default value is **disabled**.
- **name**
  Specifies a unique name for the component. This option is required for the commands **create**, **delete**, and **modify**.
- **override-connection-limit**
  Specifies, when **enabled**, that the pool member connection limits are not enforced for persisted clients. Per-virtual connection limits remain hard limits and are not disabled. The default value is **disabled**.
- **partition**
  Displays the administrative partition within which the component resides.
- **regex**
  Displays the items that match the regular expression. The regular expression must be preceded by an at sign (@[regular expression]) to indicate that the identifier is a regular expression. See **help regex** for a description of regular expression syntax.
- **timeout**
  Specifies the duration of the persistence entries. The default value is **300** seconds.
- **to-folder**
  ssl persistence profiles can be moved to any folder under **/Common**, but configuration dependencies may restrict moving the profile out of **/Common**.

See Also

create, *delete*, *edit*, glob, *list*, *virtual*, *modify*, *mv*, regex, *show*, *tmsh*

universal

Configures a universal persistence profile.

Syntax

Configure the **universal** component within the **ltm persistence** module using the syntax in the following sections.

Modify

```
create universal [name]
modify universal [name]
    app-service [[string] | none]
    defaults-from [name]
    description [string]
    match-across-pools [enabled | disabled]
    match-across-services [enabled | disabled]
    match-across-virtuals [enabled | disabled]
    method [hash | insert | passive | rewrite]
    mirror [enabled | disabled]
    override-connection-limit [enabled | disabled]
    rule [ [iRule name] | none]
    timeout [integer]
edit universal [ [ [name] | [glob] | [regex] ] ... ]
   all-properties
   non-default-properties
mv universal [ [[source-name] [destination-name]] | [[name] to-folder [folder-name]] |
[[name...name] to-folder [folder-name]] ]
    to-folder
```

Display

```
list universal
list universal [ [ [name] | [glob] | [regex] ] ... ]
show running-config universal
show running-config universal [ [ [name] | [glob] | [regex] ] ... ]
    all-properties
    non-default-properties
    one-line
    partition
```

Delete

```
delete universal [name]
```

Description

You can use the **universal** component to configure a universal persistence profile for the BIG-IP® system. With universal persistence you can write an expression that defines what to persist on in a packet. The expression, written using the same expression syntax that you use in iRules®, defines some sequence of bytes to use as a session identifier.

A persistence profile is a profile that enables persistence when you assign the profile to a virtual server. Using a persistence profile means that you do not have to write an iRule to implement a type of persistence. You can either use the default profile, or create a custom profile based on the default.

Examples

list universal

Displays all universal persistence profiles.

create universal uni_persistence defaults-from universal

Creates a custom universal persistence profile named **uni_persistence** that inherits its settings from the default universal persistence profile.

mv universal /Common/my_universal_profile to-folder /Common/my_folder

Moves a custom universal persistence profile named **my_universal_profile** to a folder named **my_folder**, where **my_folder** has already been created and exists within **/Common**.

Options

- **app-service**
  Specifies the name of the application service to which the profile belongs. The default value is **none**. **Note:** If the **strict-updates** option is **enabled** on the application service that owns the object, you cannot modify or delete the profile. Only the application service can modify or delete the profile.
- **defaults-from**
  Specifies the existing profile from which the system imports settings for the new profile. The default value is **universal**, the system default cookie persistence profile.
- **description**
  User defined description.
- **glob**
  Displays the items that match the **glob** expression. See **help glob** for a description of **glob** expression syntax.
- **match-across-pools**
  Specifies, when **enabled**, that the system can use any pool that contains this persistence record. The default value is **disabled**.

- **match-across-services**
  Specifies, when **enabled**, that all persistent connections from a client IP address, which go to the same virtual IP address, also go to the same node. The default value is **disabled**.
- **match-across-virtuals**
  Specifies, when **enabled**, that all persistent connections from the same client IP address go to the same node. The default value is **disabled**.
- **mirror**
  Specifies whether the system mirrors persistence records to the high-availability peer. The default value is **disabled**.
- **name**
  Specifies a unique name for the component. This option is required for the commands **create**, **delete**, and **modify**.
- **override-connection-limit**
  Specifies, when **enabled**, that the pool member connection limits are not enforced for persisted clients. Per-virtual connection limits remain hard limits and are not disabled. The default value is **disabled**.
- **partition**
  Displays the administrative partition within which the component resides.
- **regex**
  Displays the items that match the regular expression. The regular expression must be preceded by an at sign (@[regular expression]) to indicate that the identifier is a regular expression. See **help regex** for a description of regular expression syntax.
- **rule**
  Specifies an iRule name when you are using a rule for universal persistence.
- **timeout**
  Specifies the duration of the persistence entries. The default value is **180** seconds.
- **to-folder**
  universal persistence profiles can be moved to any folder under **/Common**, but configuration dependencies may restrict moving the profile out of **/Common**.

See Also

create, *delete*, *edit*, glob, *list*, *virtual*, *modify*, *mv*, regex, *show*, *tmsh*

67

ltm profile

- Introducing the ltm profile module
- Alphabetical list of components

Introducing the ltm profile module

You can use the tmsh components that reside within the ltm profile module to configure profiles for Local Traffic Manager™. For more information about the tmsh hierarchical structure, see Chapter 2, *Understanding and Using the Traffic Management Shell*.

Alphabetical list of components

The remainder of this chapter lists the tmsh components that are available in the ltm profile module.

analytics

Configures an analytics profile.

Syntax

Configure the **analytics** component within the **ltm profile** module using the syntax shown in the following sections.

Create/Modify

```
create analytics [name]
modify analytics [name]
    alerts [none | add | delete | modify | replace-all-with] {
      name [string] {
          app-service [[string] | none]
          granularity [application | pool-member |
            virtual-server]
          metric [average-page-load-time | average-request-throughput |
            average-response-throughput | average-server-latency |
            average-tps | max-page-load-time | max-request-throughput |
            max-server-latency | max-response-throughput | max-tps]
          sample-period [integer]
          threshold [integer]
          threshold-relation [above | below]
      }
    }
    app-service [[string] | none]
    captured-traffic-external-logging [enabled | disabled]
    captured-traffic-internal-logging [enabled | disabled]
    collect-page-load-time [enabled | disabled]
    collect-geo [enabled | disabled]
    collect-http-throughput [enabled | disabled]
    collect-ip [enabled | disabled]
    collect-max-tps-and-throughput [enabled | disabled]
    collect-methods [enabled | disabled]
    collect-response-codes [enabled | disabled]
    collect-server-latency [enabled | disabled]
    collect-subnets [enabled | disabled]
    collect-url [enabled | disabled]
    collect-user-agent [enabled | disabled]
    collect-user-sessions [enabled | disabled]
    collected-stats-external-logging [enabled | disabled]
    collected-stats-internal-logging [enabled | disabled]
    defaults-from [ analytics profile name [string] | none]
    description [string]
    external-logging-publisher [name]
    notification-by-email [enabled | disabled]
    notification-by-snmp [enabled | disabled]
    notification-by-syslog [enabled | disabled]
    notification-email-addresses [none | add | delete | modify |
      replace-all-with] { email-address [string] }
    publish-irule-statistics [enabled | disabled]
    sampling [enabled | disabled]
    session-cookie-security [always-secure | ssl-only | never-secure]
    session-timeout-minutes [integer]
    smtp-config [ smtp configuration object name ]
```

```
    subnet-masks [none | add | delete | modify |
      replace-all-with] {
      name [string] {
           subnet [IPv4/IPv6 address]
      }
    }
    traffic-capture [none | add | delete | modify |
      replace-all-with] {
      name [string] {
          app-service [[string] | none]
          captured-protocols [all | http | https]
          client-ips [none | add | delete | modify |
            replace-all-with] { ipv4.address }
          dos-activity [any | mitigated-by-dosl7]
          methods [none | add | delete | modify |
            replace-all-with] { method [string] }
          node-addresses [none | add | delete | modify |
            replace-all-with] { node }
          request-captured-parts [all | body | headers | none]
          request-content-filter-search-part [all | body | headers |
            none | uri]
          request-content-filter-search-string [none | [string]]
          response-captured-parts [all | body | headers | none]
          response-codes [none | add | delete | modify |
            replace-all-with] { response-code [integer] }
          response-content-filter-search-part [all | body |
            headers | none]
          response-content-filter-search-string [none | [string]]
          url-path-prefixes [none | add | delete | modify |
            replace-all-with] { url-path-prefix [string] }
          user-agent-substrings [none | add | delete | modify |
            replace-all-with] { user-agent-substring [string] }
          virtual-servers [none | add | delete | modify |
            replace-all-with] { virtual }
      }
    }
edit analytics [ [ [name] | [glob] | [regex] ] ... ]
    all-properties
    non-default-properties
```

Display

```
list analytics
list analytics [ [ [name] | [glob] | [regex] ] ... ]
show running-config analytics
show running-config analytics [ [ [name] | [glob] | [regex] ] ... ]
    all-properties
    non-default-properties
    one-line
    partition
```

Delete

```
delete analytics [name]
```

Description

Use the **analytics** component to create, modify, display, or delete an analytics profile for use with analytics functionality.

Examples

create analytics my_analytics_profile defaults-from analytics

Creates a custom analytics profile named **my_analytics_profile** that inherits its settings from the system default analytics profile.

list analytics

Displays the properties of all analytics profiles.

Options

- **app-service**
  Specifies the name of the application service to which the profile belongs. The default value is **none**. **Note:** If the **strict-updates** option is **enabled** on the application service that owns the object, you cannot modify or delete the profile. Only the application service can modify or delete the profile.
- **alerts**
  Adds, deletes, or replaces a set of analytics alerts. You can configure the following options for an analytics alert:
  - **app-service**
    Specifies the name of the application service to which the alert belongs. The default value is **none**. **Note:** If the **strict-updates** option is **enabled** on the application service that owns the object, you cannot modify or delete the alert. Only the application service can modify or delete the alert.
  - **granularity**
    Specifies a granularity level on which the alert is defined.
    The options are:
    - **application**
      Specifies that an alert is triggered for applications for which a **threshold** is breached.
    - **pool-member**
      Specifies that an alert is triggered for pool members for which a **threshold** is breached.
    - **virtual-server**
      Specifies that an alert is triggered for virtual servers for which a **threshold** is breached.
  - **metric**
    Specifies a metric on which the alert is defined.
    The options are:

- **average-page-load-time**
  Specifies that an alert is triggered when the average time it takes for the client to respond to a request breaches the defined threshold.
- **average-request-throughput**
  Specifies that an alert is triggered when the average number of bits per second the system processed, based on requests only, breaches the defined threshold.
- **average-response-throughput**
  Specifies that an alert is triggered when the average number of bits per second the system processed, based on responses only, breaches the defined threshold.
- **average-server-latency**
  Specifies that an alert is triggered when the average time it takes for the web server to respond to a request breaches the defined threshold.
- **average-tps**
  Specifies that an alert is triggered when the average number of transactions per second breaches the defined threshold.
- **max-page-load-time**
  Specifies that an alert is triggered when the longest time it takes for the client to respond to a request breaches the defined threshold.
- **max-request-throughput**
  Specifies that an alert is triggered when the maximum number of bits per second the system processed, based on requests only, breaches the defined threshold.
- **max-response-throughput**
  Specifies that an alert is triggered when the maximum number of bits per second the system processed, based on requests only, breaches the defined threshold.
- **max-server-latency**
  Specifies that an alert is triggered when the longest time it takes for the web server to respond to a request breaches the defined threshold.
- **max-tps**
  Specifies that an alert is triggered when the largest number of transactions per second breaches the defined threshold.

- **name**
  Specifies a unique name for an alert. This option is required for the commands create, delete, and modify.
- **sample-period**
  Specifies that the alert **metric** is triggered when the conditions that trigger the alert last a defined amount of time, measured in seconds. The default value is **300**.
- **threshold**
  Specifies the threshold that must be breached in order for the system to generate alert.

- **threshold-relation**
  Specifies whether the metric value must be below or above the **metric**.
  The options are:
  - **above**
    Specifies that an alert is issued if **metric** current value is above the **threshold**.
  - **below**
    Specifies that an alert is issued if **metric** current value is below the **threshold**.

- **captured-traffic-external-logging**
  Enables or disables the external logging of captured traffic.
- **captured-traffic-internal-logging**
  Enables or disables the internal logging of captured traffic.
- **collect-page-load-time**
  Enables or disables the collection of the page load time statistics. The page load time is the round-trip latency between client end-users and the servers, that is, the round-trip time between an end-userÐ¢¬Ä¬ôs request for a page until the time the response finishes loading.
- **collect-geo**
  Enables or disables the collection of the names of the countries from where the traffic was sent.
- **collect-http-throughput**
  Enables or disables the collection of throughput statistics. This property has been deprecated. As of v11.3.0, HTTP throughput is always collected.
- **collect-ip**
  Enables or disables the collection of client IPs statistics.
- **collect-max-tps-and-throughput**
  Enables or disables the collection of maximum TPS and throughput for all collected entities.
- **collect-methods**
  Enables or disables the collection of HTTP methods statistics.
- **collect-response-codes**
  Enables or disables the collection of response codes returned by the servers.
- **collect-server-latency**
  Enables or disables the collection of server latency statistics. This property has been deprecated. As of v11.3.0, server latency is always collected.
- **collect-subnets**
  Enables or disables the collection of client side subnets.
- **collect-url**
  Enables or disables the collection of requested URL statistics.
- **collect-user-agent**
  Enables or disables the collection of user agents.

- **collect-user-sessions**
  Enables or disables the collection of the unique user sessions.
- **collected-stats-external-logging**
  Enables or disables the external logging of the collected statistics.
- **collected-stats-internal-logging**
  Enables or disables the internal logging of the collected statistics.
- **defaults-from**
  Specifies the profile that you want to use as the parent profile. Your new profile inherits all settings and values from the parent profile specified. The default value is **analytics**.
- **description**
  User defined description.
- **external-logging-publisher**
  Specifies the external logging publisher used to send statistical data to one or more destinations.
- **glob**
  Displays the items that match the **glob** expression. See **help glob** for a description of **glob** expression syntax.
- **name**
  Specifies a unique name for the component. This option is required for the commands **create**, **delete**, and **modify**.
- **notification-by-email**
  Enables or disables sending the analytics alerts by email.
- **notification-by-snmp**
  Enables or disables sending the analytics alerts by SNMP traps. **notification-by-syslog** must be enabled.
- **notification-by-syslog**
  Enables or disables logging of the analytics alerts into the Syslog.
- **notification-email-addresses**
  Specifies which email addresses receive alerts by email when **notification-by-email** is enabled.
- **partition**
  Displays the administrative partition within which the component resides.
- **publish-irule-statistics**
  Enables or disables publishing analytics statistics for iRules.
- **sampling**
  Enables or disables transaction sampling. This attribute can be set in the default profile only. The default value is **disabled**.
- **session-cookie-security**
  Specifies the condition for adding a secure attribute to the session cookie. The options are:
  - **always**
    The secure attribute is always added to the session cookie.
  - **never**
    The secure attribute is never added to the session cookie.

- **ssl-only**
  The secure attribute is only added to the session cookie when the virtual server has a client-SSL profile. This is the default value.

- **session-timeout-minutes**
  Specifies the number of minutes of user non-activity before the system considers the session to be over.
- **smtp-config**
  Specifies the SMTP configuration to be used with analytics.
- **subnet-masks**
  Adds, deletes, or replaces predefined subnet addresses. This options defines the display names given to certain subnet addresses seen in the client IP subnets report.
  - **subnet**
    Subnet address. IPv4 addresses will be masked by 255.255.255.0. IPv6 addresses will be masked by ffff:ffff:ffff:ffff:: .
- **traffic-capture**
  Adds, deletes, or replaces an analytics traffic capture definition. You can configure the following options for an analytics traffic capture:
  - **app-service**
    Specifies the name of the application service to which the analytics traffic capture belongs. The default value is **none**. **Note:** If the **strict-updates** option is **enabled** on the application service that owns the object, you cannot modify or delete the analytics traffic capture. Only the application service can modify or delete the analytics traffic capture.
  - **captured-protocols**
    Specifies whether the system captures traffic data sent using all protocols, or only one type of protocol.
    The options are:
    - **all**
      Specifies that the system captures traffic data sent using all protocols.
    - **http**
      Specifies that the system captures traffic data sent using **http** protocol.
    - **https**
      Specifies that the system captures traffic data sent using **https** protocol.
  - **client-ips**
    Adds, deletes, or replaces a set of client IP addresses from/to which captured traffic is sent.
  - **dos-activity**
    Specifies whether the system captures traffic data mitigated by DoS Layer 7 Enforcer or regardless of DoS activity.
    The options are:
    - **any**
      Specifies that system does not filter traffic data by DoS activity.

- **mitigated-by-dosl7**
  Specifies that the system captures only traffic data mitigated by DoS Layer 7 Enforcer.

- **methods**
  Adds, deletes, or replaces a set of HTTP methods used to send requests from which traffic is captured.
- **name**
  Specifies a unique name for an analytics traffic capture. This option is required for the commands create, delete, and modify.
- **node-addresses**
  Adds, deletes, or replaces a set of node addresses from/to which captured traffic is sent.
- **request-captured-parts**
  Specifies what parts of the request data the system captures.
  The options are:
  - **all**
    Specifies that the system captures all the parts of the request data.
  - **body**
    Specifies that the system captures the body of the request data.
  - **headers**
    Specifies that the system captures the HTTP headers of the request data.
  - **none**
    Specifies that the system does not capture the request data.
- **request-content-filter-search-part**
  Specifies which part of the request is filtered by a specific string.
  The options are:
  - **all**
    Specifies that the system filters all the parts of the request data.
  - **body**
    Specifies that the system filters the body of the request data.
  - **headers**
    Specifies that the system filters the HTTP headers of the request data.
  - **none**
    Specifies that system does not filter the request data.
  - **uri**
    Specifies that the system filters the URI path component, including the query string, of the request data.
- **request-content-filter-search-string**
  Specifies the string by which a request data is filtered, or **none**.
- **response-captured-parts**
  Specifies what parts of the response data the system captures.
  The options are:
  - **all**
    Specifies that the system captures all the parts of the response data.

  - **body**
    Specifies that the system captures the body of the response data.
  - **headers**
    Specifies that the system captures the HTTP headers of the response data.
  - **none**
    Specifies that the system does not capture the response data.
- **response-codes**
  Adds, deletes, or replaces a set of HTTP response codes from which traffic is captured.
- **response-content-filter-search-part**
  Specifies which part of the response is filtered by a specific string. The options are:
  - **all**
    Specifies that the system filters all the parts of the response data.
  - **body**
    Specifies that the system filters the body of the response data.
  - **headers**
    Specifies that the system filters the HTTP headers of the response data.
  - **none**
    Specifies that system does not filter the response data.
- **response-content-filter-search-string**
  Specifies the string by which the response data is filtered, or **none**.
- **url-path-prefixes**
  Adds, deletes, or replaces a set of URL path prefixes on which traffic can be captured (both to and from).
- **user-agent-substrings**
  Adds, deletes, or replaces a set of user agent substrings on which traffic can be captured (both to and from).
- **virtual-servers**
  Adds, deletes, or replaces a set of virtual servers from/to which captured traffic is sent.

See Also

create, *delete*, *edit*, glob, *list*, *virtual*, *smtp*, *modify*, regex, *reset-stats*, *show*, *tmsh*

certificate-authority

Defines the settings necessary to authenticate the client certificate.

Syntax

Configure the **certificate-authority** within the **ltm profile** module using the syntax shown in the following sections.

Create/Modify

```
create certificate-authority [name]
modify certificate-authority [name]
    authenticate-depth
    ca-file
    crl-file
    default-name
    description
    update-crl
edit certificate-authority [ [ [name] | [glob] | [regex] ] ... ]
    all-properties
    non-default-properties
```

Display

```
list certificate-authority
list certificate-authority [ [ [name] | [glob] | [regex] ] ... ]
    app-service
    partition
show certificate-authority
show certificate-authority [ [ [name] | [glob] | [regex] ] ... ]
    all-properties
    field-fmt
 non-default-properties
    one-line
```

Description

Use the **certificate-authority** component to modify or display a certificate-authority profile.

Examples

create ltm profile certificate-authority mycaprofile { ca-file ca.crt }

Creates a certificate authority profile named mycaprofile using the system defaults.

modify ltm profile certificate-authority mycaprofile { authenticate-depth 3 }

Modifies the authenticate-depth setting to 3 for the certificate authority profile named mycaprofile.

Options

- **app-service**
  Displays the application service to which the object belongs. The default value is **none**.
  Note: If the **strict-updates** option is **enabled** on the Application Service that owns the object, you cannot modify or delete the object. Only the Application Service can modify or delete the object.
- **authenticate-depth**
  Specifies the authenticate depth. This is the client certificate chain maximum traversal depth.
- **ca-file**
  Specifies the certificate authority file name or, you can use **default** for the default certificate authority file name. Configures certificate verification by specifying a list of client or server certificate authorities that the traffic management system trusts.
- **crl-file**
  Specifies the certificate revocation list file name. You can use **default** for the default certificate revocation file name.
- **defaults-from**
  Specifies the profile that you want to use as the parent profile. Your new profile inherits all settings and values from the parent profile specified.
- **description**
  User defined description.
- **name**
  Specifies the profile instance name. This option is required for the **modify** command.
- **partition**
  Specifies the administrative partition within which the profile resides.
- **regex**
  Specifies the items that match the regular expression. The regular expression must be preceded by an at sign (@[regular expression]) to indicate that the identifier is a regular expression. See **help regex** for a description of regular expression syntax.
- **update-crl**
  Automatically updates the CRL file.

See Also

edit, glob, *list*, *modify*, regex, *show*, *tmsh*,

classification

Configures a classification profile.

Syntax

Configure the **classification** profile within the **ltm profile** module using the syntax shown in the following sections.

Modify

```
modify classification [name]
    description [string]
    smtp-server [ smtp server configuration object name ]
edit classification [ [ [name] | [glob] | [regex] ] ... ]
    all-properties
    non-default-properties
```

Display

```
list classification
list classification [ [ [name] | [glob] | [regex] ] ... ]
show running-config classification
show running-config classification [ [ [name] | [glob] | [regex] ] ... ]
    all-properties
    non-default-properties
    one-line
    partition
```

Description

Use the **classification** component to modify, or display a classification profile.

Examples

edit classification classification

Edits the classification profile named **classification**.

◆ Note

The profile name cannot be changed.

list classification

Displays the properties of the classification profile.

Options

- **description**
  User defined description.
- **glob**
  Displays the items that match the **glob** expression. See **help glob** for a description of **glob** expression syntax.
- **name**
  Specifies the profile instance name. The name must be **classification**. This option is required for the **modify** command.
- **partition**
  Specifies the administrative partition within which the profile resides.
- **regex**
  Specifies the items that match the regular expression. The regular expression must be preceded by an at sign (@[regular expression]) to indicate that the identifier is a regular expression. See **help regex** for a description of regular expression syntax.
- **smtp-server**
  Specifies the SMTP server configuration to be used with classification for sending reports via email.

See Also

edit, glob, *list*, *virtual*, *modify*, regex, *reset-stats*, *show*, *tmsh*, *smtp-server*

client-ldap

Configures an Client LDAP profile.

Syntax

Configure the **client-ldap** component within the **ltm profile** module using the syntax shown in the following sections.

Create/Modify

```
create client-ldap [name]
modify client-ldap [name]
    app-service [[string] | none]
    defaults-from [ [name] | none]
    description [string]
    activation-mode [ none | allow | require ]
edit client-ldap [ [ [name] | [glob] | [regex] ] ... ]
    all-properties
    non-default-properties
```

Display

```
list client-ldap
list client-ldap [ [ [name] | [glob] | [regex] ] ... ]
show running-config client-ldap
show running-config client-ldap [ [ [name] | [glob] | [regex] ] ... ]
    all-properties
    non-default-properties
```

Delete

```
delete client-ldap [name]
```

Description

You can use the **client-ldap** component to create, modify, display, or delete an Client LDAP profile with which you can manage Client LDAP traffic.

Examples

create client-ldap my_clientldap_profile defaults-from clientldap

Creates a custom Client LDAP profile named **my_clientldap_profile** that inherits its settings from the system default Client LDAP profile.

list client-ldap

Displays the properties of all Client LDAP profiles.

Options

- **app-service**
  Specifies the name of the application service to which the profile belongs. The default value is **none**. **Note:** If the **strict-updates** option is **enabled** on the application service that owns the object, you cannot modify or delete the profile. Only the application service can modify or delete the profile.
- **defaults-from**
  Specifies the profile that you want to use as the parent profile. Your new profile inherits all settings and values from the parent profile specified. The default value is **smtp**.
- **description**
  User defined description.
- **glob**
  Displays the items that match the **glob** expression. See **help glob** for a description of **glob** expression syntax.
- **name**
  Specifies a unique name for the component. This option is required for the commands **create**, **delete**, and **modify**.
- **regex**
  Displays the items that match the regular expression. The regular expression must be preceded by an at sign (@[regular expression]) to indicate that the identifier is a regular expression. See **help regex** for a description of regular expression syntax.
- **activation-mode**
  Sets the activation-mode STARTTLS. The options are NONE, ALLOW, or REQUIRE. The default value is REQUIRE.

See Also

create, *delete*, *edit*, glob, *list*, *virtual*, *modify*, regex, *reset-stats*, *show*, *provision*, *tmsh*

client-ssl

Configures a Client SSL profile.

Syntax

Configure the **client-ssl** component within the **ltm.profile** module using the syntax shown in the following sections.

Create/Modify

```
create client-ssl [name]
modify client-ssl [name]
    alert-timeout [indefinite | [integer] ]
    allow-non-ssl [disabled | enabled]
    app-service [[string] | none]
    authenticate [always | once]
    authenticate-depth [integer]
    ca-file [name]
    cache-size [integer]
    cache-timeout [integer]
    cert [name]
    cert-extension-includes {
      none |
      [ authority-key-identifier basic-constraints
        certificate-policies crl-distribution-points
        extended-key-usage fresh-crl issuer-alternative-name
        key-usage  subject-alternative-name
        subject-directory-attribute subject-key-identifier
      ]...
    }
    cert-key-chain [add | delete | modify | replace-all-with] {
       [ [name] ] {
           cert [name | none]
           chain [name | none]
           key [name]
           passphrase [none | [string] ]
           ocsp-stapling-params [name | none]
       }
    }
    cert-lookup-by-ipaddr-port [disabled | enabled]
    chain [name | none]
    ciphers [name | none]
    client-cert-ca [name | none]
    crl-file [name]
    defaults-from [clientssl | [name] ]
    description [string]
    destination-ip-blacklist [name]
    destination-ip-whitelist [name]
    forward-proxy-bypass-default-action [intercept | bypass]
    handshake-timeout [indefinite | [integer] ]
    hostname-blacklist [name]
    hostname-whitelist [name]
    key [ [name] | none]
    mod-ssl-methods [disabled | enabled]
    mode [disabled | enabled]
    options {
```

```
        none |
        [ all-bugfixes cipher-server-preference
          dont-insert-empty-fragments ephemeral-rsa
          microsoft-big-sslv3-buffer microsoft-sess-id-bug
          msie-sslv2-rsa-padding netscape-ca-dn-bug
          netscape-challenge-bug netscape-demo-cipher-change-bug
          netscape-reuse-cipher-change-bug no-dtls
          no-session-resumption-on-renegotiation no-ssl no-sslv2 no-sslv3
          no-tls no-tlsv1 no-tlsv1.1 no-tlsv1.2 passive-close
          pkcs1-check-1 pkcs1-check-2 single-dh-use ssleay-080-client-dh-bug
          sslref2-reuse-cert-type-bug tls-block-padding-bug tls-d5-bug
          tls-rollback-bug ]...
      }
      passphrase [none | [string] ]
      peer-cert-mode [auto | ignore | request | require]
      peer-no-renegotiate-timeout [indefinite | [integer]
      proxy-ssl [disabled | enabled]
      proxy-ssl-passthrough [disabled | enabled]
      proxy-ca-cert [name]
      proxy-ca-key [name]
      proxy-ca-lifespan [integer]
      proxy-ca-passphrase [string]
      renegotiate-max-record-delay [indefinite | [integer] ]
      renegotiate-period [indefinite | [integer] ]
      renegotiate-size [indefinite | [integer] ]
      renegotiation [disabled | enabled]
      retain-certificate [true | false]
      secure-renegotiation [request | requre | require-strict]
      max-renegotiations-per-minute [integer]
      server-name [name]
      session-mirroring [disabled | enabled]
      session-ticket [disabled | enabled]
      sni-default [true | false]
      sni-require [true | false]
      source-ip-blacklist [name]
      source-ip-whitelist [name]
      ssl-forward-proxy [disabled | enabled]
      ssl-forward-proxy-bypass [disabled | enabled]
      strict-resume [disabled | enabled]
      unclean-shutdown [disabled | enabled]
      generic-alert [disabled | enabled]
      ssl-sign-hash [any | sha1 | sha256 | sha384]
edit client-ssl [ [ [name] | [glob] | [regex] ] ... ]
      all-properties
      non-default-properties
options:
 mv client-ssl [ [[source-name] [destination-name]] | [[name] to-folder [folder-name]]
| [[name...name] to-folder [folder-name]] ]
  to-folder
reset-stats client-ssl
reset-stats client-ssl [ [ [name] | [glob] | [regex] ] ... ]
```

Display

```
list client-ssl
list client-ssl [ [ [name] | [glob] | [regex] ] ... ]
show running-config client-ssl
show running-config client-ssl [ [ [name] | [glob] | [regex] ] ... ]
      all-properties
```

```
    non-default-properties
    one-line
    partition
show client-ssl
show client-ssl [ [ [name] | [glob] | [regex] ] ... ]
    (default | exa | gig | kil | meg | peta | raw | tera | yotta | zetta)
    field-fmt
    global
```

Delete

```
delete client-ssl [name]
```

Description

You can use the **client-ssl** component to create, modify, or delete a custom Client SSL profile, or display a custom or default Client SSL profile.

Client-side profiles allow the traffic management system to handle authentication and encryption tasks for any SSL connection coming into a traffic management system from a client system.

Examples

create client-ssl my_clientssl_profile

Creates a clientssl profile named **my_clientssl_profile** using the system defaults.

create clientssl my_clientssl_profile authenticate-depth number

Creates a Client SSL profile named **my_clientssl_profile** using the system defaults, except that a user is authenticated with depth **number**.

mv client-ssl /Common/my_client-ssl_profile to-folder /Common/my_folder

Moves a custom client-ssl profile named **my_client-ssl_profile** to a folder named **my_folder**, where **my_folder** has already been created and exists within **/Common**.
=head1 OPTIONS

- **alert-timeout**
  Specifies the maximum time period in seconds to keep the SSL session active after alert message is sent. The default value is **10** seconds.
- **allow-non-ssl**
  Enables or disables non-SSL connections. Specify **enabled** when you want non-SSL connections to pass through the traffic management system as clear text. The default value is **disabled**.
- **app-service**
  Specifies the name of the application service to which the profile belongs. The default value is **none**. **Note:** If the **strict-updates** option is

enabled on the application service that owns the object, you cannot modify or delete the profile. Only the application service can modify or delete the profile.

- **authenticate**
  Specifies how often the system authenticates a user. The default value is **once**.
- **authenticate-depth**
  Specifies the authenticate depth. This is the client certificate chain maximum traversal depth. The default value is **9**.
- **ca-file**
  Specifies the certificate authority (CA) file name. Configures certificate verification by specifying a list of client or server CAs that the traffic management system trusts. The default value is **none**.
- **cache-size**
  Specifies the SSL session cache size. For client-side profiles only, you can configure timeout and size values for the SSL session cache. Because each profile maintains a separate SSL session cache, you can configure the values on a per-profile basis. The default value is **262144**.
- **cache-timeout**
  Specifies the SSL session cache timeout value. This specifies the number of usable lifetime seconds of negotiated SSL session IDs. The default value is **3600** seconds. Acceptable values are integers greater than or equal to **0** and less than or equal to **86400**.
- **cert**
  This option is **deprecated** and is maintained here for backward compatibility reasons. Please check cert-key-chain option to add certificate, key, passphrase and chain to the profile.
- **cert-extension-includes**
  Specifies the extensions of the web server certificates to be included in the generated certificates using SSL Forward Proxy. For example, { **basic-constraints** }. The default value is none. The extensions are:
  - **authority-key-identifier**
    Authority Key Identifier provides a means of identifying the public key corresponding to the private key used to sign a certificate.
  - **basic-constraints**
    Basic Constraints are used to indicate whether the certificate belongs to a CA.
  - **certificate-policies**
    Certificate Policies contain a sequence of one or more policy information terms.
  - **crl-distribution-points**
    CRL Distribution Points identify how CRL information is obtained.
  - **destination-ip-blacklist**
    Specifies the data group name of destination ip blacklist when SSL forward proxy bypass feature is enabled.

- **destination-ip-whitelist**
  Specifies the data group name of destination ip whitelist when SSL forward proxy bypass feature is enabled.
- **extended-key-usage**
  Extended Key Usage is used, typically on a leaf certificate, to indicate the purpose of the public key contained in the certificate.
- **forward-proxy-bypass-default-action**
  Specifies the SSL forward proxy bypass default action. The default option is **intercept**.
- **fresh-crl**
  Fresh CRL (a.k.a Delta CRL Distribution Point) identifies how delta CRL information is obtained.
- **hostname-blacklist**
  Specifies the data group name of hostname blacklist when SSL forward proxy bypass feature is enabled.
- **hostname-whitelist**
  Specifies the data group name of hostname whitelist when SSL forward proxy bypass feature is enabled.
- **issuer-alternative-name**
  As with **subject-alternative-name**, Issuer Alternative Name is used to associate Internet style identities with the certificate issuer.
- **key-usage**
  Key Usage provides a bitmap specifying the cryptographic operations which may be performed using the public key contained in the certificate; for example, it could indicate that the key should be used for signature but not for encipherment.
- **subject-alternative-name**
  Subject Alternative Name allows identities to be bound to the subject of the certificate. These identities may be included in addition to or in place of the identity in the subject field of the certificate.
- **subject-directory-attributes**
  Subject Directory Attributes are used to convey identification attributes (for example, nationality) of the subject.
- **subject-key-identifier**
  Subject Key Identifier provides a means of identifying certificates that contains a particular public key.

◆ **cert-key-chain**
Adds, deletes, or replaces a set of certificate, key, passphrase, chain and OCSP Stapling Parameters object. **client-ssl** profile requires at least one **cert/key** pair to work. Multiple **cert/key** types can be associated to a **client-ssl** profile using following options:

- **cert**
  Specifies the name of the certificate installed on the traffic management system for the purpose of terminating or initiating an SSL connection. You can specify the default certificate name, which is **default.crt**.

- **chain**
  Specifies or builds a certificate chain file that a client can use to authenticate the profile. The default value is **none**.
- **key**
  Specifies the name of a key file that you generated and installed on the system. When selecting this option, type a key file name or use the default value **default.key**.
- **passphrase**
  Specifies the key passphrase, if required. The default value is **none**.
- **ocsp-stapling-params**
  Specifies the OCSP Stapling Parameters object which will be used with this cert-key-chain object for a client-ssl profile. The default value is **none**.

◆ **cert-lifespan**
Specifies the lifespan of the certificate generated using the SSL forward proxy feature. The default value is **30**.

◆ **cert-lookup-by-ipaddr-port**
Specifies whether to perform certificate look up by IP address and port number.

◆ **chain**
This option is **deprecated** and is maintained here for backward compatibility reasons. Please check cert-key-chain option to add certificate, key, passphrase and chain to the profile.

◆ **ciphers**
Specifies a cipher name. The default value is **DEFAULT**, which uses the default ciphers.

◆ **client-cert-ca**
Specifies the client cert certificate authority name. The default value is **none**.

◆ **crl-file**
Specifies the certificate revocation list file name. The default value is **none**.

◆ **defaults-from**
This setting specifies the profile that you want to use as the parent profile. Your new profile inherits all settings and values from the parent profile specified. The default value is **clientssl**.

◆ **description**
User defined description.

◆ **glob**
Displays the items that match the **glob** expression. See **help glob** for a description of **glob** expression syntax.

◆ **handshake-timeout**
Specifies the handshake timeout in seconds. The default value is **10** seconds.

- **key**
  This option is **deprecated** and is maintained here for backward compatibility reasons. Please check cert-key-chain option to add certificate, key, passphrase and chain to the profile.
- **mod-ssl-methods**
  Enables or disables ModSSL method emulation. Enable this option when OpenSSL methods are inadequate, for example, when you want to use SSL compression over TLSv1. The default value is **disabled**.
- **mode**
  Specifies the profile mode, which enables or disables SSL processing. The default value is **enabled**.
- **name**
  Specifies a unique name for the component. This option is required for the commands **create**, **delete**, and **modify**.
- **options**
  Enables options, including some industry-related workarounds. Enter options inside braces, for example, **{dont-insert-empty-fragments microsoft-sess-id-bug}**.
  The default value is **dont-insert-empty-fragments**. The options are:
  - **all-bugfixes**
    This option enables the following industry-related defect workarounds: microsoft-sess-id-bug, netscape-challenge-bug, netscape-reuse-cipher-change-bug, sslref2-reuse-cert-type-bug, microsoft-big-sslv3-buffer, msie-sslv2-rsa-padding, ssleay-080-client-dh-bug, tls-d5-bug, tls-block-padding-bug, and dont-insert-empty-fragments.
    It is usually safe to use this option to enable the defect workaround options when compatibility with broken implementations is desired. It is usually safe to use this option to enable the defect workaround options when compatibility with broken implementations is desired. Note that if you edit the configuration in the Web-based configuration utility, the system expands the **all-bugfixes** syntax into each individual option.
  - **cipher-server-preference**
    When choosing a cipher, this option uses the server's preferences instead of the client references. If this option was not set, the SSL server would follow the client's references. When this option is set, the SSLv3/TLSv1 server chooses by using its own references.

◆ Note

This option has no effect. The BIG-IP system always behaves as if the option is active, even when you disable it.

  - **dont-insert-empty-fragments**
    Disables a countermeasure against an SSL 3.0/TLS 1.0 protocol vulnerability affecting CBC ciphers. These ciphers cannot be handled by certain broken SSL implementations. This option has no effect for connections using other ciphers.

- **ephemeral-rsa**
  Uses ephemeral (temporary) RSA keys when doing RSA operations. According to the specifications, this is done only when an RSA key can be used for signature operations only (namely under export ciphers with restricted RSA key length). By setting this option, you specify that you want to use ephemeral RSA keys always. This option breaks compatibility with the SSL/TLS specifications and may lead to interoperability problems with clients. Therefore, F5 Networks does not recommend this option. Use ciphers with ephemeral Diffie-Hellman (EDH) key exchange instead. This option is ignored for server-side SSL.
- **microsoft-big-sslv3-buffer**
  Enables a workaround for communicating with older Microsoft® applications that use non-standard SSL record sizes.
- **microsoft-sess-id-bug**
  Handles a Microsoft session ID problem.
- **msie-sslv2-rsa-padding**
  Enables a workaround for communicating with older Microsoft applications that use non-standard RSA key padding. This option is ignored for server-side SSL.
- **netscape-ca-dn-bug**
  Handles a defect regarding the system crashing or hanging. If the system accepts a Netscape Navigator® browser connection, demands a client cert, has a non-self-signed CA that does not have its CA in Netscape, and the browser has a certificate, the system crashes or hangs.
- **netscape-challenge-bug**
  Handles the Netscape challenge problem.
- **netscape-demo-cipher-change-bug**
  Manipulates the SSL server session resumption behavior to mimic that of certain Netscape servers (see the Netscape reuse cipher change bug workaround description). Note that F5 Networks does not recommend this option for normal use. It is ignored for server-side SSL.
- **netscape-reuse-cipher-change-bug**
  Handles a defect within Netscape-Enterprise/2.01 (https://merchant.neape.com), only appearing when connecting through SSLv2/v3 then reconnecting through SSLv3. In this case, the cipher list changes.
  First, a connection is established with the RC4-MD5 cipher list. If it is then resumed, the connection switches to using the DES-CBC3-SHA cipher list. However, according to RFC 2246, (section 7.4.1.3, cipher suite) the cipher list should remain RC4-MD5.
  As a workaround, you can attempt to connect with a cipher list of DES-CBC-SHA:RC4-MD5 and so on. For some reason, each new connection uses the RC4-MD5 cipher list, but any re-connection attempts to use the DES-CBC-SHA cipher list. Thus Netscape, when reconnecting, always uses the first cipher in the cipher list.

- **no-session-resumption-on-renegotiation**
  When performing renegotiation as an SSL server, this option always starts a new session (that is, session resumption requests are only accepted in the initial handshake). The system ignores this option for server-side SSL.
- **no-ssl**
  Do not use any version of the SSL protocol.
- **no-sslv2**
  Do not use the SSLv2 protocol.
- **no-sslv3**
  Do not use the SSLv3 protocol.
- **no-tls**
  Do not use any version of the TLS protocol.
- **no-tlsv1**
  Do not use the TLSv1.0 protocol.
- **no-tlsv1.1**
  Do not use the TLSv1.1 protocol.
- **no-tlsv1.2**
  Do not use the TLSv1.2 protocol.
- **no-dtls**
  Do not use any version of the DTLS protocol.
- **passive-close**
  Specifies how to handle passive closes.
- **none**
  Disables all workarounds. Note that F5 Networks does not recommend this option.
- **pkcs1-check-1**
  This debugging option deliberately manipulates the PKCS1 padding used by SSL clients in an attempt to detect vulnerability to particular SSL server vulnerabilities. Note that F5 Networks does not recommend this option for normal use. The system ignores this option for client-side SSL.
- **pkcs1-check-2**
  This debugging option deliberately manipulates the PKCS1 padding used by SSL clients in an attempt to detect vulnerability to particular SSL server vulnerabilities. Note that F5 Networks does not recommend this option for normal use. The system ignores this option for client-side SSL.
- **single-dh-use**
  Creates a new key when using temporary/ephemeral DH parameters. This option must be used to prevent small subgroup attacks, when the DH parameters were not generated using strong primes (for example. when using DSA-parameters). If strong primes were used, it is not strictly necessary to generate a new DH key during each handshake, but F5 Networks recommends it. Enable the Single DH Use option whenever temporary or ephemeral DH parameters are used.

- **ssleay-080-client-dh-bug**
  Enables a workaround for communicating with older SSLeay-based applications that specify an incorrect Diffie-Hellman public value length. This option is ignored for server-side SSL.
- **sslref2-reuse-cert-type-bug**
  Handles the SSL reuse certificate type problem.
- **tls-block-padding-bug**
  Enables a workaround for communicating with older TLSv1-enabled applications that use incorrect block padding.
- **tls-d5-bug**
  This option is a workaround for communicating with older TLSv1-enabled applications that specify an incorrect encrypted RSA key length. This option is ignored for server-side SSL.
- **tls-rollback-bug**
  Disables version rollback attack detection. During the client key exchange, the client must send the same information about acceptable SSL/TLS protocol levels as it sends during the first hello. Some clients violate this rule by adapting to the server's answer. For example, the client sends an SSLv2 hello and accepts up to SSLv3.1 (TLSv1), but the server only processes up to SSLv3. In this case, the client must still use the same SSLv3.1 (TLSv1) announcement. Some clients step down to SSLv3 with respect to the server's answer and violate the version rollback protection. The system ignores this option for server-side SSL.

◆ **partition**
Displays the administrative partition within which the profile resides.

◆ **passphrase**
This option is **deprecated** and is maintained here for backward compatibility reasons. Please check cert-key-chain option to add certificate, key, passphrase and chain to the profile.

◆ **peer-cert-mode**
Specifies the peer certificate mode. The default value is **ignore**.

◆ **peer-no-renegotiate-timeout**Specifies the timeout in seconds when the server sends Hello Request and waits for ClientHello before it sends Alert with fatal alert. You can also specify indefinite. The default is **10** seconds.

◆ **proxy-ca-cert**
Specifies the name of the certificate file that is used as the certification authority certificate when SSL forward proxy feature is enabled. The certificate should be generated and installed by you on the system. When selecting this option, type a certificate file name.

◆ **proxy-ca-key**
Specifies the name of the key file that is used as the certification authority key when SSL forward proxy feature is enabled. The key should be generated and installed by you on the system. When selecting this option, type a key file name.

- **proxy-ca-passphrase**
  Specifies the passphrase of the key file that is used as the certification authority key when SSL forward proxy feature is enabled. When selecting this option, type the passphrase corresponding to the selected proxy-ca-key.
- **proxy-ssl**
  Enabling this option requires a corresponding server ssl profile with **proxy-ssl** enabled to perform transparent SSL decryption. This allows further modification of application traffic within an SSL tunnel while still allowing the server to perform necessary authorization, authentication, auditing steps.
- **proxy-ssl-passthrough**
  Enabling this option requires a corresponding server ssl profile with **proxy-ssl-passthrough** enabled. This allows Proxy SSL to passthrough the traffic when ciphersuite negotiated between the client and server is not supported. The default option is **disabled**.
- **regex**
  Displays the items that match the regular expression. The regular expression
  must be preceded by an at sign (@[regular expression]) to indicate that the
  identifier is a regular expression. See **help regex** for a description of regular expression syntax.
- **renegotiate-max-record-delay**
  Specifies the maximum number of SSL records that the traffic management system can receive before it renegotiates an SSL session. After the system receives this number of SSL records, it closes the connection. This setting applies to client profiles only. The default value is **indefinite**.
- **renegotiate-period**
  Specifies the number of seconds required to renegotiate an SSL session. The default value is **indefinite**.
- **renegotiate-size**
  Specifies the size of the application data, in megabytes, that is transmitted over the secure channel. If the size of the data is higher than this value, the traffic management system must renegotiate the SSL session. The default value is **indefinite**.
- **renegotiation**
  Specifies whether renegotiations are enabled. The default value is **enabled**.
  When renegotiations are disabled, and the system is acting as an SSL server, and
  a COMPAT or NATIVE cipher is negotiated, the system will abort the connection.
  Additionally, when renegotiations are disabled, and the system is acting as an
  SSL client, the system will ignore the server's HelloRequest messages.

- **retain-certificate**
  APM module requires storing certificate in SSL session. When set to false,
  certificate will not be stored in SSL session. The default value is **true**.
- **generic-alert**
  Enables or disables generic-alert. The default option is **enabled**, which causes the SSL profile to use generic alert number. Conversely, you can specify **disabled** to cause SSL profile to use alert number defined in RFC5246/RFC6066 strictly.
- **secure-renegotiation**
  Specifies the secure renegotiation mode. The default value is **require**. When secure renegotiation is required, any client attempting to renegotiate that does not support secure renegotiation will have its connection aborted. When secure renegotiation is set to **require-strict**, any client attempting to connect that does not support secure renegotiation will have its initial handshake denied. When secure renegotiation is set to **request**, unpatched clients will be permitted to renegotiate. This setting is NOT recommended however, as it is subject to active man-in-the-middle attacks.
- **max-renegotiations-per-minute**
  Specifies the maximum number of renegotiation attempts allowed in a minute. The default value is **5**.
- **server-name**
  Specifies the server names to be matched with SNI (server name indication) extension information in ClientHello from a client connection. Wildcard is supported by using wildcard character "*" to match multiple names.
- **sni-default**
  When true, this profile is the default SSL profile when the server name in a client connection does not match any configured server names, or a client connection does not specify any server name at all.
- **sni-require**
  When this option is enabled, a client connection that does not specify a known server name or does not support SNI extension will be rejected.
- **ssl-sign-hash**
  Specifies SSL sign hash algorithm which is used to sign and verify SSL Server Key Exchange and Certificate Verify messages for the specified SSL profiles. The default value is **sha1**.
- **strict-resume**
  Enables or disables strict-resume. The default option is **disabled**, which causes the SSL profile to resume an uncleanly shut down SSL session. Conversely, you can specify **enabled** to prevent an SSL session from being resumed after an unclean shutdown.
- **unclean-shutdown**
  By default, the SSL profile performs unclean shutdowns of all SSL connections, which means that underlying TCP connections are closed

without exchanging the required SSL shutdown alerts. If you want to force the SSL profile to perform a clean shutdown of all SSL connections, set this option to **disabled**.

- **session-mirroring**
  Enables or disables the mirroring of sessions to high availability peer. By default, this setting is disabled, which causes the system to not mirror ssl sessions.
- **session-ticket**
  Enables or disables session-ticket. The default option is **disabled**, which causes the SSL profile not to use session ticket per RFC 5077. Conversely, you can specify **enabled** to cause SSL profile to use session ticket per RFC 5077.
- **source-ip-blacklist**
  Specifies the data group name of source ip blacklist when SSL forward proxy bypass feature is enabled.
- **source-ip-whitelist**
  Specifies the data group name of source ip whitelist when SSL forward proxy bypass feature is enabled.
- **ssl-forward-proxy**
  Enables or disables SSL forward proxy feature. The default option is **disabled**. Conversely, you can specify **enabled** to use the SSL Forward Proxy Feature.
- **ssl-forward-proxy-bypass**
  Enables or disables SSL forward proxy bypass feature. The default option is **disabled**. Conversely, you can specify **enabled** to use the SSL Forward Proxy Bypass Feature.
- **to-folder**
  client-ssl profiles can be moved to any folder under **/Common**, but configuration dependencies may restrict moving the profile out of **/Common**.

See Also

create, *delete*, *edit*, glob, *list*, *virtual*, *modify*, *mv*, regex, *reset-stats*, *show*, *tmsh*

dhcpv4

Configures a Dynamic Host Configuration Protocol (DHCP) profile.

Syntax

Configure the **dhcpv4** profile within the **ltm profile** module using the syntax shown in the following sections.

Create/Modify

```
create dhcpv4 [name]
modify dhcpv4 [name]
    app-service [[string] | none]
    defaults-from [[name] | none]
    mode [relay | forwarding]
    description [string]
    idle-timeout [immediate | indefinite | integer]
    default-lease-time [integer]
    transaction-timeout [integer]
    authentication {
        enabled [true | false]
        virtual [[string] | none]
        user-name {
            format [mac-address | mac-and-relay-option | relay-option | tcl-snippet]
            suboption-id1 [integer]
            suboption-id2 [integer]
            separator1 [[string] | none]
            separator2 [[string] | none]
             tcl [[string] | none]
       }
    }
    subscriber-discovery {
        enabled [true | false]
       subscriber-id {
            format [mac-address | mac-and-relay-id | tcl-snippet]
            suboption-id1 [integer]
            suboption-id2 [integer]
            separator1 [[string] | none]
            separator2 [[string] | none]
            tcl [[string] | none]
       }
    }
    relay-agent-id {
        add [true | false]
        remove [true | false]
        suboption {
            id1 [integer]
            id2 [integer]
            value1 [string | none]
            value2 [string | none]
       }
    }
    ttl-value [[integer]| none]
    ttl-dec-value [ by-0 | by-1 | by-2 | by-4 ]
```

```
edit dhcpv4 [ [name]  ... ]
    all-properties
    non-default-properties
reset-stats dhcpv4
reset-stats dhcpv4 [ [ [name] | [regex] ] ... ]
```

Display

```
list dhcpv4
list dhcpv4 [ [ [name] | [regex] ] ... ]
show running-config dhcpv4
show running-config dhcpv4
  [ [ [name] | [regex] ] ... ]
    all-properties
    non-default-properties
    one-line
    partition
show dhcpv4
show dhcpv4 [ [ [name] | [regex] ] ... ]
    (default | exa | gig | kil | meg | peta | raw | tera | yotta | zetta)
    field-fmt
    global
```

Delete

```
delete dhcpv4 [name]
```

Description

You can use the **dhcpv4** profile to manage DHCPv4 network traffic.

Examples

create dhcpv4 my_dhcpv4_profile defaults-from dhcpv4

Creates a custom DHCPv4 profile named **my_dhcpv4_profile** that inherits its settings from the system default DHCPv4 profile.

list dhcpv4 all-properties

Displays all properties for all DHCPv4 profiles.

```
create dhcpv4 new_dhcpv4_profile {
   mode relay
   idle-timeout 120
   transaction-timeout 45
   default-lease-time 3600
   ttl-value 0
   ttl-dec-value by-2
   subscriber-discovery {
      enabled true
      subscriber-id {
         format mac-and-relay-option
         suboption-id1 1
```

```
            separator1 -
        }
    }
    authentication {
        enabled true
        virtual new_authen_vs
        user-name {
            format mac-and-relay-option
            suboption-id1 1
            separator1 -
        }
    }
    relay-agent-id {
        add false
        remove true
    }
}
```

Creates a DHCPv4 profile named **new_dhcpv4_profile** with idle-timeout value of <120 seconds>, transaction-timeout of <45 seconds>, default-lease-time of **3600 seconds**, and ttl-dec-value of **2**. The BIG-IP virtual will work in relay mode, with subscriber discovery enabled and configured with the subscriber-id format set to mac-and-relay-option and configured to use only suboption 1 (the first suboption ID) of the relay-agent info option (option 82) and to use the **-** to concatenate the MAC address to the first suboption ID. The authentication is enabled and its user-name equals the subscriber-id and the
authentication virtual name is new_authen_vs. It also does not add relay agent option 82 but removed it (if exists) from the server-to-client messages.

Options

- **app-service**
  Specifies the name of the application service to which the profile belongs. The default value is **none**. **Note:** If the **strict-updates** option is **enabled** on the application service that owns the object, you cannot modify or delete the profile. Only the application service can modify or delete the profile.
- **default-lease-time**
  Provides the default value in seconds of DHCPv4 lease time in case it was missing in the client-server exchange. The default is **86400**.
- **defaults-from**
  Specifies the profile that you want to use as the parent profile. Your new profile inherits all settings and values from the parent profile. The default value is **dhcpv4**.
- **description**
  User defined description.

- **mode**
  Specifies the operation mode of the DHCP virtual. If the virtual to run in relay mode, then it means that it is acting as a standard DHCPv4 relay agent. This means that the relay will change some of the DHCPv4 packet fields before sending it to either the client or server. The forwarding mode is similar to relay except that the virtual will not modify the standard fields, instead it will forward the message from client to server and vice-versa. The default is **relay**.
- **idle-timeout**
  Specifies the number of seconds that a connection is idle before the connection is eligible for deletion. The default value is **60** seconds.
- **transaction-timeout**
  Specifies DHCPv4 transaction timeout, in seconds. The transactions should complete within the timeout specified. If a transaction does not complete for any reason, it is removed. The default value is 45 seconds.
- **authentication**
  Manages the subscriber authentication attributes.
  - **enabled**
    To enable or disable subscriber authentication. If enabled, then user has to fill the following fields. Default is **false**.
  - **virtual**
    Specifies the authentication virtual server name.
  - **user-name**
    Manages the authentication user name's attributes. The user-name is what will be used to authenticate the DHCP client.
    - **format**
      Specifies the user-name format. The options are: MAC address, MAC + relay-agent option, relay-agent option or tcl-snippet. The concatenation symbol is defined as **separator1**.
    - **suboption-id1**
      The relay-agent option (option 82) first suboption ID. The default is **1**.
    - **suboption-id2**
      The relay-agent option (option 82) second suboption ID. The default is **2**.
    - **separator1**
      A string that is used to concatenate the MAC address and the relay-agent info option (option 82) to create the authentication user-name. The default is @.
    - **separator2**
      A string that is used to concatenate the relay-agent info option (option 82) suboptions 1 and 2 to create the authentication user-name. The default is @.
    - **tcl-snippet**
      A tcl snippet to format the user name. This value will be taken into account only if the format value was chosen to be **tcl-snippet**.

- **subscriber-discovery**
  Manages the subscriber discovery attributes.
  - **enabled**
    To enable or disable subscriber discovery. If enabled, then user has to fill the following fields. Default is **false**.
  - **subscriber-id**
    Manages the subscriber-id attributes. The subscriber-id is used by SPM to create, delete and update subscriber sessions.
    - **format**
      Specifies the subscriber-id format. The options are: MAC address, MAC + relay-agent option, relay-agent option or tcl-snippet. The concatenation symbol is defined as **separator1**.
    - **suboption-id1**
      The relay-agent info option (option 82) first suboption ID. The default is **1**.
    - **suboption-id2**
      The relay-agent info option (option 82) second suboption ID. The default is **2**.
    - **separator1**
      A string that is used to concatenate the MAC address and the relay-agent info option (option 82) to create the subscriber-id. The default is @.
    - **separator2**
      A string that is used to concatenate the relay-agent info option (option 82) suboptions 1 and 2 to create the subscriber-id. The default is @.
    - **tcl-snippet**
      A tcl snippet to format the subscriber-id. This value will be taken into account only if the format value was chosen to be **tcl-snippet**.
- **relay-agent-id**
  Manages the relay agent information option (option 82) attributes. As a relay, the DHCP virtual can insert this option.
  - **add**
    Specifies if the user wants the DHCP relay agent to insert option 82 or not. Default is **false**.
  - **remove**
    Specifies if the user wants the DHCP relay agent to remove option 82 from the server-to-client traffic or not. Default is **false**.
  - **suboptions**
    Manages the inserted relay agent information option (option 82) suboptions. We allow only two suboptions to be inserted.
    - **id1**
      An integer to represent the first suboption ID. Default is **1**.
    - **value1**
      A string to represent the first suboption value.

  - **id2**
    An integer to represent the second suboption ID. Default is **2**.
  - **value2**
    A string to represent the second suboption value.

- **ttl-value**
  Specifies the ttl absolute value that the user may want to set for each outgoing DHCP packet. Default is **0**; and in this case, we use the **ttl-dec-value** field.
- **ttl-dec-value**
  Specifies the amount that the DHCP virtual will use to decrement the ttl for each outgoing DHCP packet. Default is **by-1**.

See Also

create, *delete*, *edit*, *ltm profile*, *virtual*, *modify*, *show*, dhcpv6 profile, *reset-stats*, *tmsh*

dhcpv6

Configures a Dynamic Host Configuration Protocol for IPv6 (DHCPv6) profile.

Syntax

Configure the **dhcpv6** profile within the **ltm profile** module using the syntax shown in the following sections.

Create/Modify

```
create dhcpv6 [name]
modify dhcpv6 [name]
    app-service [[string] | none]
    defaults-from [[name] | none]
    mode [relay | forwarding]
    description [string]
    idle-timeout [immediate | indefinite | integer]
    default-lease-time [integer]
    transaction-timeout [integer]
    authentication {
        enabled [true | false]
        virtual [[string] | none]
        user-name {
            format [mac-address | option37 | mac-and-option37 | option38 |
mac-and-option38 | option37-and-option38 | mac-and-option37-and-option38 |
tcl-snippet]
            separator1 [[string] | none]
            separator2 [[string] | none]
            tcl [[string] | none]
       }
    }
    subscriber-discovery {
        enabled [true | false]
       subscriber-id {
            format [mac-address | option37 | mac-and-option37 | option38 |
mac-and-option38 | option37-and-option38 | mac-and-option37-and-option38 |
tcl-snippet]
            separator1 [[string] | none]
            separator2 [[string] | none]
            tcl [[string] | none]
       }
    }
    remote-id-option {
       add [true | false]
       remove [true | false]
       enterprise-number [integer]
       value [string | none]
    }
    subscriber-id-option {
       add [true | false]
       remove [true | false]
       value [string | none]
    }
```

```
edit dhcpv6 [ [name]  ... ]
    all-properties
    non-default-properties
reset-stats dhcpv6
reset-stats dhcpv6 [ [ [name] | [regex] ] ... ]
```

Display

```
list dhcpv6
list dhcpv6 [ [ [name] | [regex] ] ... ]
show running-config dhcpv6
show running-config dhcpv6
  [ [ [name] | [regex] ] ... ]
    all-properties
    non-default-properties
    one-line
    partition
show dhcpv6
show dhcpv6 [ [ [name] | [regex] ] ... ]
    (default | exa | gig | kil | meg | peta | raw | tera | yotta | zetta)
    field-fmt
    global
```

Delete

```
delete dhcpv6 [name]
```

Description

You can use the **dhcpv6** profile to manage DHCPv6 network traffic.

Examples

create dhcpv6 my_dhcpv6_profile defaults-from dhcpv6

Creates a custom DHCPv6 profile named **my_dhcpv6_profile** that inherits its settings from the system default DHCPv6 profile.

list dhcpv6 all-properties

Displays all properties for all DHCPv6 profiles.

```
create dhcpv6 new_dhcpv6_profile {
   mode relay
   idle-timeout 120
   transaction-timeout 45
   default-lease-time 3600
   subscriber-discovery {
      enabled true
      subscriber-id {
         format mac-and-option37
         separator1 @
      }
   }
```

```
    authentication {
        enabled true
        virtual new_authen_vs
        user-name {
            format mac-and-option37
            separator1 @
        }
    }
    remote-id-option {
        add false
        remove true
    }
    subscriber-id-option {
        add false
        remove true
    }
}
```

Creates a DHCPv6 profile named **new_dhcpv6_profile** with idle-timeout value of <120 seconds>, transaction-time out of <45 seconds> and default-lease-time of **3600 seconds**. The BIG-IP virtual will work in relay mode, with subscriber discovery enabled and configured with the subscriber-id format set to mac-and-option37 (remote-id relay agent option) and to use the @ to concatenate both MAC address and option 37. The authentication is enabled and its user-name equals the subscriber-id and the authentication virtual name is new_authen_vs. It also does not add either option 37 or options 38 (remote-id option and subscriber-id option) but remove them (if exists) from the server-to-client messages.

Options

- **app-service**
  Specifies the name of the application service to which the profile belongs. The default value is **none**. **Note:** If the **strict-updates** option is **enabled** on the application service that owns the object, you cannot modify or delete the profile. Only the application service can modify or delete the profile.
- **default-lease-time**
  Provides the default value in seconds of DHCPv6 lease time in case it was missing in the client-server exchange. The default is **86400**.
- **defaults-from**
  Specifies the profile that you want to use as the parent profile. Your new profile inherits all settings and values from the parent profile. The default value is **dhcpv6**.
- **description**
  User defined description.
- **mode**Specifies the operation mode of the DHCP virtual. If the virtual to run in relay mode, then it means that it is acting as a standard DHCPv6 relay agent. This means that the relay will encapsulate the original

messages into one of the relay messages before it send it to the server or the client. In the forwarding mode, the virtual will just forward the message to either the server or the client. The default is **relay**.

- **idle-timeout**
  Specifies the number of seconds that a connection is idle before the connection is eligible for deletion. The default value is **60** seconds.
- **transaction-timeout**
  Specifies DHCPv6 transaction timeout, in seconds. The transactions should complete within the timeout specified. If a transaction does not complete for any reason, it is removed. The default value is 45 seconds.
- **authentication**
  Manages the subscriber authentication attributes.
  - **enabled**
    To enable or disable subscriber authentication. If enabled, then user has to fill the following fields. Default is **false**.
  - **virtual**
    Specifies the authentication virtual server name.
  - **user-name**
    Manages the authentication user name's attributes. The user-name is what will be used to authenticate the DHCP client.
    - **format**
      Specifies the user-name format. The options are: MAC address, option37, MAC + option37, option38, MAC + option38, option37 + option38, mac + option37 + option38 tcl-snippet. The concatenation symbols are defined as **separator1** and **seprator2**.
    - **separator1**
      A string that is used to concatenate the MAC address and the first two strings of the authentication user-name. The default is @.
    - **separator2**
      A string that is used to concatenate the MAC address and the second two strings of the authentication user-name. The default is @.
    - **tcl-snippet**
      A tcl snippet to format the user name. This value will be taken into account only if the format value was chosen to be **tcl-snippet**.
- **subscriber-discovery**
  Manages the subscriber discovery attributes.
  - **enabled**
    To enable or disable subscriber discovery. If enabled, then user has to fill the following fields. Default is **false**.
  - **subscriber-id**
    Manages the subscriber-id attributes. The subscriber-id is used by SPM to create, delete and update subscriber sessions.

- **format**
  Specifies the user-name format. The options are: MAC address, option37, MAC + option37, option38, MAC + option38, option37 + option38, mac + option37 + option38 tcl-snippet. The concatenation symbols are defined as **separator1** and **seprator2**.
- **separator1**
  A string that is used to concatenate the first two strings of the subscriber-id. The default is @.
- **separator2**
  A string that is used to concatenate the second two strings of the subscriber-id. The default is @.
- **tcl-snippet**
  A tcl snippet to format the subscriber-id. This value will be taken into account only if the format value was chosen to be **tcl-snippet**.

◆ **remote-id-option**
Manages the DHCPv6 relay agent remote-id option (option 37) attributes. As a relay, the DHCP virtual can insert or remove this option.

- **add**
  Specifies if the user wants the DHCP relay agent to insert option 37 or not. Default is **false**.
- **remove**
  Specifies if the user wants the DHCP relay agent to remove option 37 from the server-to-client traffic or not. Default is **false**.
- **enterprise-number**
  Specifies the enterprise number of the inserted remote-id option (option 37).
- **value**
  A string to represent the remote-id option value.

◆ **subscriber-id-option**
Manages the DHCPv6 relay agent subscriber-id option (option 38) attributes. As a relay, the DHCP virtual can insert or remove this option.

- **add**
  Specifies if the user wants the DHCP relay agent to insert option 38 or not. Default is **false**.
- **remove**
  Specifies if the user wants the DHCP relay agent to remove option 38 from the server-to-client traffic or not. Default is **false**.
- **value**
  A string to represent the subscriber-id option value.

See Also

create, *delete*, *edit*, *ltm profile*, *virtual*, *modify*, *show*, dhcpv6 profile, *reset-stats*, *tmsh*

diameter

Configures a profile to manage Diameter network traffic.

Syntax

Configure the **diameter** component within the **ltm profile** module using the syntax in the following sections.

Create/Modify

```
create diameter [name]
modify diameter [name]
    app-service [[string] | none]
    connection-prime [disabled | enabled]
    defaults-from [name]
    description [string]
    destination-realm [string]
    handshake-timeout [number]
    host-ip-rewrite [disabled | enabled]
    max-retransmit-attempts [number]
    max-watchdog-failure [number]
    origin-host-to-client [string]
    origin-host-to-server [string]
    origin-realm-to-client [string]
    origin-realm-to-server [string]
    overwrite-destination-host [disabled | enabled]
    parent-avp [ [number] | [string] ]
    persist-avp [ [number] | [string] ]
    reset-on-timeout [disabled | enabled]
    retransmit-timeout [number]
    subscriber-aware [disabled | enabled]
    watchdog-timeout [number]
mv diameter [ [[source-name] [destination-name]] | [[name] to-folder [folder-name]] |
[[name...name] to-folder [folder-name]] ]
    to-folder
edit diameter [ [ [name] | [glob] | [regex] ] ... ]
    all-properties
    non-default-properties
reset-stats diameter
reset-stats diameter [ [ [name] | [glob] | [regex] ] ... ]
```

Display

```
list diameter
list diameter [ [ [name] | [glob] | [regex] ] ... ]
show running-config diameter
show running-config diameter [ [ [name] | [glob] | [regex] ] ... ]
    all-properties
    non-default-properties
    one-line
    partition
```

```
show diameter
show diameter [ [ [name] | [glob] | [regex] ] ... ]
    (default | exa | gig | kil | meg | peta | raw | tera | yotta | zetta)
    field-fmt
    global
```

Delete

```
delete diameter [name]
```

Description

You can use the **diameter** component to configure a profile to manage Diameter network traffic.

Examples

create diameter my_diameter_profile defaults-from diameter

Creates a Diameter profile named **my_diameter_profile** that inherits its settings from the system default Diameter profile.

list diameter

Displays the properties of all Diameter profiles.

mv diameter /Common/my_diameter_profile to-folder /Common/my_folder

Moves a custom diameter profile named **my_diameter_profile** to a folder named **my_folder**, where **my_folder** has already been created and exists within **/Common**.

Options

- **app-service**
  Specifies the name of the application service to which the profile belongs. The default value is **none**. **Note:** If the **strict-updates** option is **enabled** on the application service that owns the object, you cannot modify or delete the profile. Only the application service can modify or delete the profile.
- **connection-prime**
  When **enabled**, and the system receives a capabilities exchange request from the client, the system will establish connections and perform handshaking with all the servers prior to sending the capabilities exchange answer to the client. The default value is **disabled**.
- **defaults-from**
  Specifies the profile that you want to use as the parent profile. Your new profile inherits all settings and values from the parent profile specified. The default value is **diameter**.

- **description**
  User defined description.
- **destination-realm**
  This attribute has been deprecated as of BIG-IP v11.3.0. Specifies the realm to which messages are routed. A value of **none** indicates that the **destination-realm** option is disabled. The default value is **none**.
  You can specify a fully qualified domain name as an ASCII string. For more information about this option, see **RFC 3588 section 6.6**.
- **glob**
  Displays the items that match the **glob** expression. See **help glob** for a description of **glob** expression syntax.
- **handshake-timeout**
  Specifies the handshake timeout in seconds. This setting specifies the maximum number of seconds that a connection can be idle after the capabilities exchange request was sent to the server.The default value is **10**. The system will reset the connection after it has timed out.
  You can specify a numeric value in the range **0** to **4294967295**. The recommended value is in the range of **5** to **30**
- **host-ip-rewrite**
  When **enabled** and the message is a capabilities exchange request or capabilities exchange answer, rewrite the host-ip-address attribute with the system's egress IP address. The default value is **enabled**.
- **max-retransmit-attempts**
  Specifies the maximum number of retransmit attempts. This setting specifies the maximum number of attempts that BIG-IP will take to retransmit the request messages if it does not receive the corresponding answer messages. If retransmit is unsuccessful, after maximum attempts, BIG_IP will send an error response. The default value is **1**.
  You can specify a numeric value in the range **0** to **4294967295**. The recommended value is in the range of **1** to **10**
- **max-watchdog-failure**
  Specifies the maximum number of device watchdog failures that the traffic management system can take before it tears down the connection. After the system receives this number of device watchdog failures, it closes the connection. The default value is **10**.
  You can specify a numeric value in the range **0** to **4294967295**.
- **name**
  Specifies a unique name for the component. This option is required for the commands **create**, **delete**, and **modify**.
- **origin-host**
  This attribute has been deprecated as of BIG-IP v11.3.0. Please use, **origin-host-to-client** or **origin-host-to-server**. Specifies the origin host of BIG-IP. The origin-host is used to overwrite the server's actual origin host attribute when it responds to the client. A value of **none** indicates that origin-host is disabled. The default value is **none**.
  You can specify an ASCII string as a FQDN. See RFC 3588 section 6.3.

- **origin-host-to-client**
  Specifies the origin host to client of BIG-IP. The origin-host-to-client is used to overwrite the server's actual origin host attribute when it responds to the client. A value of **none** indicates that origin-host-to-client is disabled. The default value is **none**.
  You can specify an ASCII string as a FQDN. See RFC 3588 section 6.3.
- **origin-host-to-server**
  Specifies the origin host to server of BIG-IP. The origin-host-to-server is used to overwrite the client's actual origin host attribute when it responds to the server. A value of **none** indicates that origin-host-to-server is disabled. The default value is **none**.
  You can specify an ASCII string as a FQDN. See RFC 3588 section 6.3.
- **origin-realm**
  This attribute has been deprecated as of BIG-IP v11.3.0. Please use, **origin-realm-to-client** or **origin-realm-to-server**. Specifies the origin realm of BIG-IP. The origin-realm is used to overwrite the server's actual origin realm attribute when it responds to the client. A value of **none** indicates that origin-realm is disabled. The default value is **none**.
  You can specify an ASCII string as a FQDN. See RFC 3588 section 6.4.
- **origin-realm-to-client**
  Specifies the origin realm of BIG-IP. The origin-realm-to-client is used to overwrite the server's actual origin realm attribute when it responds to the client. A value of **none** indicates that origin-realm-to-client is disabled. The default value is **none**.
  You can specify an ASCII string as a FQDN. See RFC 3588 section 6.4.
- **origin-realm-to-server**
  Specifies the origin realm to server of BIG-IP. The origin-realm-to-server is used to overwrite the client's actual origin realm attribute when it responds to the server. A value of **none** indicates that origin-realm-to-server is disabled. The default value is **none**.
  You can specify an ASCII string as a FQDN. See RFC 3588 section 6.4.
- **overwrite-destination-host**
  This attribute has been deprecated as of BIG-IP v11.3.0. When you enable this option, the system replaces the value of the destination host field in the Diameter header with the BIG-IP® pool member address. When you disable this option, the system does not modify the destination host field. The default value is **enabled**.
- **parent-avp**
  Specifies the name of the Diameter attribute that the system uses to indicate if the **persist-avp** option is embedded in a grouped avp. A value of **none** indicates that the value of the **persist-avp** option is not embedded in a grouped avp. The default value is **none**.
  You can specify an ASCII string or a numeric ID in the range **1** to **4294967295**. Acceptable strings can be found in RFC 3588 section 4.5.
- **partition**
  Displays the administrative partition within which the profile resides.
- **persist-avp**
  Specifies the name of the Diameter attribute that the system persists on. A value of **none** indicates that persistence is disabled. The default value

is **session-id**.
You can specify an ASCII string or a numeric ID in the range **1** to **4294967295**. Acceptable strings can be found in RFC 3588 section 4.5.

- **regex**
  Displays the items that match the regular expression. The regular expression must be preceded by an at sign (@[regular expression]) to indicate that the identifier is a regular expression. See **help regex** for a description of regular expression syntax.
- **reset-on-timeout**
  When it is **enabled** and the watchdog failures exceed the max watchdog failure, the system resets the connection. The default value is **enabled**.
- **retransmit-timeout**
  Specifies the retransmit timeout in seconds. This setting specifies the number of seconds to retransmit the request messages if BIG-IP does not receive the corresponding answer messages . The default value is **10**.
  You can specify a numeric value in the range **0** to **4294967295**. The recommended value is in the range of **5** to **30**
- **subscriber-aware**
  When you enable this option, the system extracts available subscriber information, such as phone number or phone model, from diameter authentication and/or accounting packets. The system then cross-references this information with the source IP address of the flows traversing the system. When you disable this option, the system does not extract subscriber information from the diameter packets. The default value is **disabled**.
- **to-folder**
  diameter profiles can be moved to any folder under **/Common**, but configuration depenedencies may restrict moving the profile out of **/Common**.
- **watchdog-timeout**
  Specifies the watchdog timeout in seconds. This setting specifies the number of seconds that a connection is idle before the device watchdog request is sent. The default value is **0**, which means BIG-IP will not send a device watchdog request to either client or server side.
  You can specify a numeric value in the range **0** to **4294967295**. The recommended value is in the range of **6** to **30**

See Also

create, *delete*, *edit*, glob, *list*, *virtual*, *modify*, *mv*, regex, *reset-stats*, *show*, *tmsh*

dns

Configures a Domain Name System (DNS) profile.

Syntax

Configure the **dns** component within the **ltm profile** module using the syntax in the following sections.

Create/Modify

```
create dns [name]
modify dns [name]
    app-service [[string] | none]
    defaults-from [ [name] | none]
    description [string]
    dns64 [disabled | secondary | immediate | v4-only]
    dns64-additional-section-rewrite [disabled | v6-only | v4-only | any]
    dns64-prefix [IPv6 prefix]
    avr-dnsstat_sample_rate [integer]
    enable-dnssec [no | yes]
    enable-dns-express [no | yes]
    enable-gtm [no | yes]
    enable-logging [no | yes]
    enable-rapid-response [no | yes]
    log-profile [ [name] | none]
    process-rd [no | yes]
    rapid-response-last-action [allow | drop | noerror | nxdomain | refuse | truncate]
    unhandled-query-action [allow | drop | hint | noerror | reject]
    use-local-bind [no | yes]
edit dns [ [ [name] | [glob] | [regex] ] ... ]
    all-properties
    non-default-properties
mv dns [ [[source-name] [destination-name]] | [[name] to-folder [folder-name]] |
[[name...name] to-folder [folder-name]] ]
    to-folder
reset-stats dns
reset-stats dns [ [ [name] | [glob] | [regex] ] ... ]
```

Display

```
list dns
list dns [ [ [name] | [glob] | [regex] ] ... ]
show running-config dns
show running-config dns [ [ [name] | [glob] | [regex] ] ... ]
    all-properties
    non-default-properties
    one-line
    partition
```

Delete

```
delete dns [name]
```

Description

You can use this component to create, modify, display, or delete a DNS profile to define how the BIG-IP system handles DNS traffic. You can also display and reset DNS profile statistics.

Examples

create dns my_dns_profile defaults-from dns

Creates a DNS profile named **my_dns_profile** that inherits its settings from the system default DNS profile.

list dns

Displays the properties of all DNS profiles.

mv dns /Common/my_dns_profile to-folder /Common/my_folder

Moves a custom dns profile named **my_dns_profile** to a folder named **my_folder**, where **my_folder** has already been created and exists within **/Common**.

Options

- **app-service**
  Specifies the name of the application service to which the profile belongs. The default value is **none**. **Note:** If the **strict-updates** option is **enabled** on the application service that owns the object, you cannot modify or delete the profile. Only the application service can modify or delete the profile.
- **avr-dnsstat-sample-rate**
  Sets AVR DNS statistics rate. The default value is **0**, which means AVR DNS statistics is disabled. If the sampling rate is set to **1**, each query will be sent to the analytics database. If the sampling rate is set to an integer **N**, every **N** th query will be sent and the analytics database will count it **N** times. When sampling rate is greater than one, the statistics will be inaccurate if the traffic volume is low. However, when the traffic volume is high, the system performance will benefit from sampling and the inaccuracy will be negligible. Also be aware that analytics database has its own internal sampling mechanism. The sampling rate does not apply to DNS firewall statistics. AVR DNS statistics contain query name, query type, virtual server IP and client IP.
- **defaults-from**
  Specifies the profile that you want to use as the parent profile. Your new profile inherits all settings and values from the parent profile specified. The default value is **dns**.
- **description**
  User defined description.
- **dns64**
  Sets DNS64 mapping mode. The default value is **disabled**.

- **dns64-additional-section-rewrite**
  Sets DNS64 additional section rewriting. For AAAA and A records in additional section, this field specifies how they are being rewritten. The default value is **disabled**.
- **dns64-prefix**
  Specifies DNS64 mapping IPv6 prefix.
- **enable-dnssec**
  Indicates whether to perform DNS Security Extension (DNSSEC) operations on the DNS packet, for example, respond to DNSKEY queries; add RRSIGs to response.
- **enable-dns-express**
  Indicates whether the dns-express service is enabled. The service handles zone transfers from the primary DNS server.
- **enable-gtm**
  Indicates whether the Global Traffic Manager handles DNS resolution for DNS queries and responses that contain Wide IP names. The default value is **yes**.
- **enable-logging**
  Indicates whether to enable high speed logging for DNS queries and responses or not. Default value is **no**. When it is set to **yes**, a DNS profile must be configured with a log-profile.
- **enable-rapid-response**
  Indicates whether to allow queries to be answered by Rapid Response. The default value is **no**. When enabled, if the query name matches a GTM Wide IP name and GTM is enabled on this profile, the DNS query will bypass Rapid Response.
- **glob**
  Displays the items that match the **glob** expression. See **help glob** for a description of **glob** expression syntax.
- **log-profile**
  Specifies the DNS logging profile used to configure what events get logged and their message format.
- **name**
  Specifies a unique name for the component. This option is required for the commands **create**, **delete**, and **modify**.
- **partition**
  Displays the administrative partition within which the profile resides.
- **process-rd**
  Indicates whether to process clientside DNS packets with Recursion Desired set in the header. The default value is **yes**. If set to **no**, processing of the packet will be subject to the **unhandled-query-action** option.
- **rapid-response-last-action**
  Specifies what action to take when Rapid Response is enabled and the incoming query has not matched a DNS-Express Zone. Default is **drop**. Option **allow** sends non-matching queries up the regular packet

processing path. All other options result in a response returned immediately to the client: **truncate** (truncate), **nxdomain** (non-existent name), **noerror** (no data), **refuse** (REFUSED return code).

- **regex**
  Displays the items that match the regular expression. The regular expression must be preceded by an at sign (@[regular expression]) to indicate that the identifier is a regular expression. See **help regex** for a description of regular expression syntax.
- **to-folder**
  dns profiles can be moved to any folder under **/Common**, but configuration dependencies may restrict moving the profile out of **/Common**.
- **unhandled-query-action**
  Specifies the action to take when a query does not match a Wide IP or a DNS Express Zone. The default value is **allow**.
- **use-local-bind**
  Indicates whether non-GTM and non-dns-express requests should be forwarded to the local BIND.

See Also

create, *delete*, *edit*, glob, *list*, *virtual*, *modify*, *mv*, regex, *reset-stats*, *show*, *tmsh*

dns-logging

Configures a domain name service logging (DNS Logging) profile.

Syntax

Configure the **dns-logging** component within the **ltm profile** module using the syntax in the following sections.

Create/Modify

```
create dns-logging [name]
modify dns-logging [name]
    enable-query-logging [no | yes]
    enable-response-logging [no | yes]
    include-complete-answer [no | yes]
    include-query-id [no | yes]
    include-source [no | yes]
    include-timestamp [no | yes]
    include-view [no | yes]
    log-publisher [name]
edit dns-logging [ [ [name] | [glob] | [regex] ] ... ]
    all-properties
    non-default-properties
mv dns-logging [ [[source-name] [destination-name]] | [[name] to-folder [folder-name]]
| [[name...name] to-folder [folder-name]] ]
    to-folder
```

Display

```
list dns-logging
list dns-logging [ [ [name] | [glob] | [regex] ] ... ]
    all-properties
    non-default-properties
    one-line
    partition
```

Delete

```
delete dns-logging [name]
```

Description

You can use this component to create, modify, display, or delete a DNS logging profile, to enable query or response logging, and to define the format of messages themselves.

Examples

list dns-logging

Displays the properties of all DNS logging profiles.

create dns-logging my_dns_log_profile enable-query-logging yes log-publisher my_pub include-query-id yes

Creates a DNS logging profile with query logging enabled. Messages will be sent to publisher my_pub. Messages will contain the query ID.

mv dns-logging /Common/my_dns_logging_profile to-folder /Common/my_folder

Moves a custom dns-logging profile named **my_dns_logging_profile** to a folder named **my_folder**, where **my_folder** has already been created and exists within **/Common**.

Options

- **enable-query-logging**
  Log the contents of DNS queries. The default value for this option is yes.
- **enable-response-logging**
  Log the contents of DNS responses. The default value is no.
- **glob**
  Displays the items that match the **glob** expression. See **help glob** for a description of **glob** expression syntax.
- **include-complete-answer**
  Selects whether all the resource records are included in response log messages. The default value is yes (complete-answer).
- **include-query-id**
  Selects whether the query id sent by the client is included in the query and response log messages. The default value is no.
- **include-source**
  Selects whether the message originator is included in the query and response log messages. The default value is yes.
- **include-timestamp**
  Selects whether the time stamp of the message is included in the query and response log messages. The default value is yes. You may or may not need this depending on whether the destination log servers prepend a time stamp to messages.
- **include-view**
  Selects whether the view is included in the query log messages. The default value is yes.
- **log-publisher**
  Specifies the log publisher used to deliver messages to one or more destinations. This option must be specified.
- **regex**
  Displays the items that match the regular expression. The regular expression must be preceded by an at sign (@[regular expression]) to indicate that the identifier is a regular expression. See **help regex** for a description of regular expression syntax.

- **to-folder**
  dns-logging profiles can be moved to any folder under **/Common**, but configuration depenedencies may restrict moving the profile out of **/Common**.

See Also

create, *delete*, *edit*, glob, *list*, *modify*, *mv*, regex, *dns*, *tmsh*

fasthttp

Configures a Fast HTTP profile.

Syntax

Modify the **fasthttp** component within the **ltm profile** module using the syntax shown in the following sections.

Create/Modify

```
create fasthttp [name]
modify fasthttp [name]
    app-service [[string] | none]
    client-close-timeout [integer]
    connpool-idle-timeout-override [integer]
    connpool-max-reuse [integer]
    connpool-max-size [integer]
    connpool-min-size [integer]
    connpool-replenish [disabled | enabled]
    connpool-step [integer]
    defaults-from [ [name]  | none]
    description [string]
    force-http-10-response [disabled | enabled]
    hardware-syn-cookie [disabled | enabled]
    header-insert [none | [string] ]
    http-11-close-workarounds [disabled | enabled]
    idle-timeout [integer]
    insert-xforwarded-for [disabled | enabled]
    layer-7 [disabled | enabled]
    max-header-size [integer]
    max-requests [integer]
    mss-override [integer]
    reset-on-timeout [disabled | enabled]
    server-close-timeout [integer]
    server-sack [disabled | enabled]
    server-timestamp [disabled | enabled]
    receive-window-size [65535 - 2^31 bytes for window scale enabling]
    unclean-shutdown [disabled | enabled]
mv fasthttp [ [[source-name] [destination-name]] | [[name] to-folder [folder-name]] |
[[name...name] to-folder [folder-name]] ]
    to-folder
edit fasthttp [ [ [name] | [glob] | [regex] ] ... ]
    all-properties
    non-default-properties
reset-stats fasthttp
reset-stats fasthttp [ [ [name] | [glob] | [regex] ] ... ]
```

Display

```
list fasthttp
list fasthttp [ [ [name] | [glob] | [regex] ] ... ]
show running-config fasthttp
show running-config fasthttp [ [ [name] | [glob] | [regex] ] ... ]
    all-properties
```

```
    non-default-properties
    one-line
    partition
show fasthttp
show fasthttp [ [ [name] | [glob] | [regex] ] ... ]
    (default | exa | gig | kil | meg | peta | raw | tera | yotta | zetta)
    field-fmt
    global
```

Delete

```
delete fasthttp [name]
```

Description

You can use this component to create, modify, display, or delete a Fast HTTP profile. This profile provides the ability to accelerate certain HTTP connections such as banner ads.

Examples

create fasthttp my_fast_http_profile defaults-from fasthttp

Creates a Fast HTTP profile named **my_fast_http_profile** that inherits its settings from the system default Fast HTTP profile.

mv fasthttp /Common/my_fasthttp_profile to-folder /Common/my_folder

Moves a custom fasthttp profile named **my_fasthttp_profile** to a folder named **my_folder**, where **my_folder** has already been created and exists within **/Common**.

show fasthttp

Displays fasthttp profile statistics in the system default units.

Options

- **app-service**
  Specifies the name of the application service to which the profile belongs. The default value is **none**. **Note:** If the **strict-updates** option is **enabled** on the application service that owns the object, you cannot modify or delete the profile. Only the application service can modify or delete the profile.
- **client-close-timeout**
  Specifies the number of seconds after which the system closes a client connection, when the system either receives a client FIN packet or sends a FIN packet. This option overrides the **idle-timeout** option. The default value is **5**.

- **server-sack**
  Specifies whether to support server sack option in cookie response by default. The default value is **disabled**.
- **server-timestamp**
  Specifies whether to support server timestamp option in cookie response by default. The default value is **disabled**.
- **receive-window-size**
  Specifies the window size to use, minimum and default to 65535 bytes, the maximum is 2^31 for window scale enabling.
- **connpool-idle-timeout-override**
  Specifies the number of seconds after which a server-side connection in a OneConnect™ pool is eligible for deletion, when the connection has no traffic. This option overrides the **idle-timeout** option. The default value is **0** (zero) seconds, which disables the override setting.
- **connpool-max-reuse**
  Specifies the maximum number of times that the system can re-use a current connection. The default value is **0** (zero).
- **connpool-max-size**
  Specifies the maximum number of connections to a load balancing pool. A value of **0** (zero) specifies that a pool can accept an unlimited number of connections. The default value is **2048**.
- **connpool-min-size**
  Specifies the minimum number of connections to a load balancing pool. The default value of **0** (zero) specifies that there is no minimum.
- **connpool-replenish**
  When enabled, the system replenishes the number of connections to a load balancing pool to the number of connections that existed when the server closed the connection to the pool. The default value is **enabled**. When disabled, the system replenishes the connection that was closed by the server, only when there are fewer connections to the pool than the number of connections set in the **connpool-min-size** option.
- **connpool-step**
  Specifies the increment at which the system makes additional connections available, when all available connections are in use. The default value is **4**.
- **defaults-from**
  Specifies the profile that you want to use as the parent profile. Your new profile inherits all settings and values from the parent profile specified. The default value is **fasthttp**.
- **description**
  User defined description.
- **force-http10-response**
  Specifies whether to rewrite the HTTP version in the status line of the server to HTTP 1.0 to discourage the client from pipelining or chunking data. The default value is **disabled**.

- **glob**
  Displays the items that match the **glob** expression. See **help glob** for a description of **glob** expression syntax.
- **hardware-syn-cookie**
  Specifies whether or not to use hardware SYN Cookie when cross system limit. The default value is **disabled**
- **header-insert**
  Specifies a string that the system inserts as a header in an HTTP request. If the header exists already, the system does not replace it. The default value is **none**.
- **http11-close-workarounds**
  Enables or disables HTTP 1.1 close workarounds. The default value is **disabled**.
- **idle-timeout**
  Specifies the number of seconds after which a connection is eligible for deletion, when the connection has no traffic. The default value is **300** seconds.
- **insert-xforwarded-for**
  Specifies whether the system inserts the **XForwarded For** header in an HTTP request with the client IP address, to use with connection pooling. The options are:
  - **disabled**
    Specifies that the system does not insert the **XForwarded For** header.
  - **enabled**
    Specifies that the system inserts the **XForwarded For** header with the client IP address.
- **layer7**
  When **enabled**, the system parses HTTP data in the stream. Disable this option if you want to use the performance HTTP profile to shield against denial-of-service attacks against non-HTTP protocols. The default value is **enabled**.
- **max-header-size**
  Specifies the maximum amount of HTTP header data that the system buffers before making a load balancing decision. The default value is **32768**.
- **max-requests**
  Specifies the maximum number of requests that the system can receive on a client connection, before the system closes the connection. The default value of **0** specifies that requests are not limited.
- **mss-override**
  Specifies a maximum segment size (MSS) override for server connections. The default value is **0** (zero), which corresponds to an MSS of 1460. You can specify any integer between **536** and **1460**.
- **name**
  Specifies a unique name for the component. This option is required for the commands **create**, **delete**, and **modify**.

- **partition**
  Displays the administrative partition within which the component resides.
- **regex**
  Displays the items that match the regular expression. The regular expression must be preceded by an at sign (@[regular expression]) to indicate that the identifier is a regular expression. See **help regex** for a description of regular expression syntax.
- **reset-on-timeout**
  When enabled, the system sends a TCP RESET packet when a connection times out, and deletes the connection. The default value is **enabled**.
- **server-close-timeout**
  Specifies the number of seconds after which the system closes a client connection, when the system either receives a client FIN packet or sends a FIN packet. This option overrides the value of the **idle-timeout** option. The default value is **5**.
- **to-folder**
  fasthttp profiles can be moved to any folder under **/Common**, but configuration depenedencies may restrict moving the profile out of **/Common**.
- **unclean-shutdown**
  Specifies how the system handles closing a connection. The options are:
  - **disabled**
    Prevents an unclean shutdown of a client connection. This is the default value.
  - **enabled**
    Specifies to permit an unclean shutdown of a client connection.
  - **fast**
    Specifies that the system sends a RESET packet to close the connection only if the client attempts to send further data after the response has completed.

See Also

create, *delete*, *edit*, glob, *list*, *virtual*, *modify*, *mv*, regex, *reset-stats*, *show*, *tmsh*

fastl4

Configures a Fast Layer 4 profile.

Syntax

Configure the **fastl4** component within the **ltm profile** module using the syntax shown in the following sections.

Create/Modify

```
create fastl4 [name]
modify fastl4 [name]
    app-service [[string] | none]
    defaults-from [ [name] | none]
    description [string]
    hardware-syn-cookie [disabled | enabled]
    idle-timeout [immediate | indefinite | [integer] ]
    ip-tos-to-client [ [integer] | pass-through]
    ip-tos-to-server [ [integer] | pass-through]
    keep-alive-interval [integer]
    link-qos-to-client [ [integer] | pass-through]
    link-qos-to-server [ [integer] | pass-through]
    priority-to-client [ [integer] | pass-through]
    priority-to-server [ [integer] | pass-through]
    loose-close [disabled | enabled]
    loose-initialization [disabled | enabled]
    mss-override [integer]
    pva-acceleration [full | none | partial | guaranteed ]
    pva-dynamic-client-packets [integer ]
    pva-dynamic-server-packets [integer ]
    pva-offload-dynamic [ enabled | disabled ]
    pva-offload-state [embryonic | establish]
    pva-flow-aging [enabled | disabled]
    pva-flow-evict [enabled | disabled]
    reassemble-fragments [disabled | enabled]
    reset-on-timeout [disabled | enabled]
    rtt-from-client [disabled | enabled]
    rtt-from-server [disabled | enabled]
    server-sack [disabled | enabled]
    server-timestamp [disabled | enabled]
    receive-window-size [65535 - 2^31 bytes for window scale enabling]
    software-syn-cookie [disabled | enabled]
    syn-cookie-whitelist [disabled | enabled]
    tcp-close-timeout [immediate | indefinite | [integer] ]
    tcp-generate-is  [disabled | enabled]
    tcp-handshake-timeout [immediate | indefinite | [integer] ]
    tcp-strip-sack [disabled | enabled]
    tcp-timestamp-mode [preserve | rewrite | strip]
    tcp-wscale-mode [preserve | rewrite | strip]
    late-binding [enabled | disabled]
    explicit-flow-migration [enabled | disabled]
    client-timeout [integer]
    timeout-recovery [ disconnect | fallback ]
mv fastl4 [ [[source-name] [destination-name]] | [[name] to-folder [folder-name]] |
[[name...name] to-folder [folder-name]] ]
    to-folder
```

```
edit fastl4 [ [ [name] | [glob] | [regex] ] ... ]
    all-properties
    non-default-properties
reset-stats fastl4
reset-stats fastl4 [ [ [name] | [glob] | [regex] ] ... ]
```

Display

```
list fastl4
list fastl4 [ [ [name] | [glob] | [regex] ] ... ]
show running-config fastl4
show running-config fastl4
  [ [ [name] | [glob] | [regex] ] ... ]
    all-properties
    non-default-properties
    one-line
    partition
show fastl4
show fastl4 [ [ [name] | [glob] | [regex] ] ... ]
    (default | exa | gig | kil | meg | peta | raw | tera | yotta | zetta)
    field-fmt
    global
```

Delete

```
delete fastL4 [name]
```

Description

You can use this component to create, modify, display, or delete a Fast Layer 4 profile. The Fast L4 profile is the default profile that the system uses when you create a basic configuration for non-UDP (User Datagram Protocol) traffic.

Any changes you make to an active Fast L4 profile (one that is in use by a virtual server) take effect after the value of the **idle-timeout** option has passed. That means new connections are affected by the profile change immediately. However, for the new values to take effect, old connections need to be either aged out or closed. =head1 EXAMPLES

create fastl4 my_fastl4_profile defaults-from fastl4

Creates a custom Fast Layer 4 profile named **my_fastl4_profile** that inherits its settings from the system default Fast L4 profile.

mv fastl4 /Common/my_fastl4_profile to-folder /Common/my_folder

Moves a custom fastl4 profile named **my_fastl4_profile** to a folder named **my_folder**, where **my_folder** has already been created and exists within **/Common**.

Please refer to the mv manual page for examples on how to use the mv command.

show fastl4

Displays statistics for all Fast Layer 4 profiles.

Options

- **app-service**
  Specifies the name of the application service to which the profile belongs. The default value is **none**. **Note:** If the **strict-updates** option is **enabled** on the application service that owns the object, you cannot modify or delete the profile. Only the application service can modify or delete the profile.
- **defaults-from**
  Specifies the profile that you want to use as the parent profile. Your new profile inherits all settings and values from the parent profile specified. The default value is **fastl4**.
- **description**
  User defined description.
- **glob**
  Displays the items that match the **glob** expression. See **help glob** for a description of **glob** expression syntax.
- **hardware-syn-cookie**
  Enables or disables hardware SYN cookie support when PVA10 is present on the system. The default value is **disabled**.
  Note that when you set the **hardware-syn-cookie** option to **enabled**, you may also want to set the following **bigdb** database variables using the **db** component, based on your requirements:
  - **pva.SynCookies.Full.ConnectionThreshold (default: 500000)**
  - **pva.SynCookies.Assist.ConnectionThreshold (default: 500000)**
  - **pva.SynCookies.ClientWindow (default: 0)**
- **idle-timeout**
  Specifies the number of seconds that a connection is idle before the connection is eligible for deletion. The default value is **300** seconds. You can also specify **immediate** or **indefinite**.
  When you specify an **idle-timeout** for the Fast L4 profile, for the profile to work properly, the value needs to be greater than the bigdb database variable **Pva.Scrub_time_in_msec**.
- **ip-tos-to-client**
  Specifies an IP Type of Service (ToS) number for the client-side. This option specifies the ToS level that the traffic management system assigns to IP packets when sending them to clients. The default value is **65535**, which indicates, do not modify.
- **ip-tos-to-server**
  Specifies an IP ToS number for the server side. This option specifies the ToS level that the traffic management system assigns to IP packets when sending them to servers. The default value is **65535**, which indicates, do not modify.

- **keep-alive-interval**
  Specifies the keep-alive probe interval, in seconds. The default value is **disabled** (0 seconds).
- **link-qos-to-client**
  Specifies a Link Quality of Service (QoS) (VLAN priority) number for the client side. This option specifies the QoS level that the system assigns to packets when sending them to clients. The default value is **65535**, which indicates, do not modify.
- **link-qos-to-server**
  Specifies a Link QoS (VLAN priority) number for the server side. This option specifies the QoS level that the system assigns to packets when sending them to servers. The default value is **65535**, which indicates, do not modify.
- **priority-to-client**
  Specifies internal packet priority for the client side. This option specifies the internal packet priority that the system assigns to packets when sending them to clients. The default value is **65535**, which indicates, do not modify.
- **link-qos-to-server**
  Specifies internal packet priority for the server side. This option specifies the internal packet priority that the system assigns to packets when sending them to servers. The default value is **65535**, which indicates, do not modify.
- **loose-close**
  Specifies that the system closes a loosely-initiated connection when the system receives the first FIN packet from either the client or the server. The default value is **disabled**.
- **loose-initialization**
  Specifies that the system initializes a connection when it receives any Transmission Control Protocol (TCP) packet, rather than requiring a SYN packet for connection initiation. The default value is **disabled**.
- **mss-override**
  Specifies a maximum segment size (MSS) override for server connections. Note that this is also the MSS advertised to a client when a client first connects.
  The default value is **0** (zero), which disables this option. You can specify an integer from **256** to **9162**.
- **name**
  Specifies a unique name for the component. This option is required for the commands **create**, **delete**, and **modify**.
- **partition**
  Displays the administrative partition within which the component resides.
- **pva-acceleration**
  Specifies the Packet Velocity® ASIC acceleration policy. The default value is **full**. guaranteed is the low latency enhancement, full and partial has same effect for ePVA platforms.

- **pva-dynamic-client-packets**
  Specifies the number of client packets before dynamic ePVA hardware re-offloading occurs. The valid value is 0~10. The default value is 2.
- **pva-dynamic-server-packets**
  Specifies the number of server packets before dynamic ePVA hardware re-offloading occurs. The valid value is 0~10. The default value is 2.
- **pva-offload-dynamic**
  Specifies whether PVA flow dynamic offloading is enabled or not. The default is enabled.
  For a flow or flow(s) in a connection to be offloaded to ePVA hardware, both the client (pva-dynamic-client-packets) and server (pva-dynamic-server-packets) flow packets setting need to be satisfied. If only one direction packets need to be taken into consideration, the other direction packets should set to zero.
- **pva-offload-state**
  Specifies at what stage the ePVA performs hardware offload. The default value is **embryonic** and implies at TCP CSYN or the first client UDP packet. **establish** implies TCP 3WAY handshaking or UDP CS round trip are confirmed.
- **pva-flow-aging**
  Specifies if automatic aging from ePVA flow cache upon inactive and idle for a period, default to **enabled**.
- **pva-flow-evict**
  Specifies if this flow can be evicted upon hash collision with a new flow learn snoop request, defaults to **enabled**.
- **reassemble-fragments**
  Specifies whether to reassemble fragments. The default value is **disabled**.
- **regex**
  Displays the items that match the regular expression. The regular expression must be preceded by an at sign (@[regular expression]) to indicate that the identifier is a regular expression. See **help regex** for a description of regular expression syntax.
- **reset-on-timeout**
  Specifies whether you want to reset connections on timeout. The default value is **enabled**.
- **rtt-from-client**
  Enables or disables the TCP timestamp options to measure the round trip time to the client. The default value is **disabled**.
- **rtt-from-server**
  Enables or disables the TCP timestamp options to measure the round trip time to the server. The default value is **disabled**.
- **server-sack**
  Specifies whether to support server sack option in cookie response by default. The default value is **disabled**.

- **server-timestamp**
  Specifies whether to support server timestamp option in cookie response by default. The default value is **disabled**.
- **receive-window-size**
  Specifies the window size to use, minimum and default to 65535 bytes, the maximum is 2^31 for window scale enabling.
- **software-syn-cookie**
  Enables or disables software SYN cookie support when PVA10 is not present on the system. The default value is **disabled**.
- **syn-cookie-whitelist**
  Specifies whether or not to use a SYN Cookie WhiteList when doing software SYN Cookies. This means not doing a SYN Cookie for the same src IP address if it has been done already in the previous tm.flowstate.timeout (30) seconds. The default value is **disabled**.
- **tcp-close-timeout**
  Specifies a TCP close timeout in seconds. You can also specify immediate or indefinite. The default value is **5** seconds.
- **tcp-generate-isn**
  Specifies whether you want to generate TCP sequence numbers on all SYNs that conform with RFC1948, and allow timestamp recycling. The default value is **disabled**.
- **tcp-handshake-timeout**
  Specifies a TCP handshake timeout in seconds. You can also specify immediate or indefinite. The default value is **5** seconds.
- **tcp-strip-sack**
  Specifies whether you want to block the TCP SackOK option from passing to the server on an initiating SYN. The default value is **disabled**.
- **tcp-timestamp-mode**
  Specifies how you want to handle the TCP timestamp. The default value is **preserve**.
- **tcp-wscale-mode**
  Specifies how you want to handle the TCP window scale. The default value is **preserve**.
- **late-binding**
  Specifies whether to enable or disable intelligent selection of a back-end server pool. The default value is **disabled**. With this option enabled, an iRule can read a Layer 7 (FIX) packet to select a server pool, and then can send the FIX stream down to the ePVA. The ePVA then manages the FIX stream at a low latency, for as long as the stream persists. To keep the latency low, the BIG-IP software does not examine any more Layer-7 data in that FIX stream.
  If you enable this option, you also need a FIX profile in the Performance FastL4 Virtual Server configuration.
- **explicit-flow-migration**
  Specifies whether to have the iRule code determine exactly when the FIX stream drops down to the ePVA hardware. The default value is **disabled**. The explicit flow migration state indicates whether connections are

automatically migrated into the ePVA hardware (disabled), or the iRule must explicitly migrate them with the BIGTCP::release_flow command (enabled).

- **client-timeout**
  Specifies late binding client timeout in seconds. This is the number of seconds allowed for a client to transmit enough data to select a server pool. If this timeout expires, the **timeout-recovery** option dictates whether to drop the connection or fallback to the normal FastL4 load-balancing method to pick a server pool. The default timeout is 30 seconds.
- **timeout-recovery**
  Specifies late binding timeout recovery mode. This is the action to take when late binding timeout occurs on a connection. This could be **disconnect** if only the L7 iRule actions are acceptable to pick a server or **fallback** if the normal FastL4 load-balancing methods are acceptable to pick a server. The default action is to **disconnect**.
- **to-folder**
  fastl4 profiles can be moved to any folder under **/Common**, but configuration depenedencies may restrict moving the profile out of **/Common**.

See Also

create, *delete*, *edit*, glob, *list*, *virtual*, *modify*, *mv*, regex, *reset-stats*, *show*, *tmsh*

fix

Configures an Financial Information eXchange Protocol (FIX) profile.

Syntax

Configure the **fix** component within the **ltm profile** module using the syntax shown in the following sections.

Create/Modify

```
create fix [name]
modify fix [name]
    app-service [[string] | none]
    error-action [drop_connection | dont_forward]
    full-logon-parsing [true | false]
    message-log-publisher [publisher]
    quick-parsing [true | false]
    statistics-sample-interval [integer]
    report-log-publisher [publisher]
    response-parsing [true | false]
    sender-tag-class {{[sender-id] [class name]}...}
edit fix [ [ [name] | [glob] | [regex] ] ... ]
    all-properties
    non-default-properties
reset-stats fix
reset-stats fix [ [ [name] | [glob] | [regex] ] ... ]
```

Display

```
list fix
list fix [ [ [name] | [glob] | [regex] ] ... ]
show running-config fix
show running-config fix [ [ [name] | [glob] | [regex] ] ... ]
    all-properties
    non-default-properties
    one-line
    partition
show fix
show fix [ [ [name] | [glob] | [regex] ] ... ]
    (default | exa | gig | kil | meg | peta | raw | tera | yotta | zetta)
    field-fmt
```

Delete

```
delete fix [name]
```

Description

You can use the **fix** component to manage an Financial Information eXchange Protocol profile.

Examples

create fix my_fix defaults-from fix

Creates an financial information exchange protocol profile named **my_fix** using the system defaults.

create fix my_fix { }

Creates an financial information exchange protocol profile named **my_fix**.

- **app-service**
  Specifies the name of the application service to which this object belongs. The
  default value is **none**.
  Note: If the **strict-updates** option is **enabled** on the application service that owns the object, you cannot modify or delete this object. Only the application
  service can modify or delete this object.
- **defaults-from**
  Specifies the profile that you want to use as the parent profile. Your new profile inherits all of the settings and values from the specified parent profile. The default value is **none**.
- **error-action**
  Specifies the error handling method.
- **full-logon-parsing**
  Enable or disable logon message is always fully parsed.
- **message-log-publisher**
  Specifies the publisher for message logging.
- **quick-parsing**
  Enable or disable quick parsing which parses the basic standard fields and validates message length and checksum.
- **statistics-sample-interval**
  Specifies the sample interval in seconds of the message rate.
- **response-parsing**
  Enable or disable response parsing which parses the messages from FIX server.
- **report-log-publisher**
  Specifies the publisher for error message and status report.
- **partition**
  Specifies the administrative partition within which the profile resides.
- **sender-tag-class**
  Specifies the tag substitution map between sender id and tag substitution data group.

See Also

create, *delete*, *edit*, glob, *list*, *virtual*, *modify*, regex, *reset-stats*, *show*, *tmsh*, *fix*

ftp

Configures an FTP profile.

Syntax

Configure the **ftp** component within the **ltm profile** module using the syntax shown in the following sections.

Create/Modify

```
create ftp [name]
modify ftp [name]
    app-service [[string] | none]
    defaults-from [ [name] | none]
    description [string]
    port [name]
    security [disabled | enabled]
    translate-extended [disabled | enabled]
    inherit-parent-profile [disabled | enabled]
    log-publisher [log publisher name | none]
    log-profile [log profile name | none]
mv ftp [ [[source-name] [destination-name]] | [[name] to-folder [folder-name]] |
[[name...name] to-folder [folder-name]] ]
    to-folder
edit ftp [ [ [name] | [glob] | [regex] ] ... ]
    all-properties
    non-default-properties
```

Display

```
list ftp
list ftp [ [ [name] | [glob] | [regex] ] ... ]
show running-config ftp
show running-config ftp [ [ [name] | [glob] | [regex] ] ... ]
    all-properties
    non-default-properties
    one-line
    partition
```

Delete

```
delete ftp [name]
```

Description

Use this command to create, modify, display, or delete an FTP profile with which you can manage FTP traffic.

Examples

create ftp my_ftp_profile defaults-from ftp

Creates a custom FTP profile named **my_ftp_profile** that inherits its settings from the system default FTP profile.

list ftp

Displays the properties of all FTP profiles.

mv ftp /Common/my_ftp_profile to-folder /Common/my_folder

Moves a custom ftp profile named **my_ftp_profile** to a folder named **my_folder**, where **my_folder** has already been created and exists within **/Common**.

Options

- **app-service**
  Specifies the name of the application service to which the profile belongs. The default value is **none**. **Note:** If the **strict-updates** option is **enabled** on the application service that owns the object, you cannot modify or delete the profile. Only the application service can modify or delete the profile.
- **defaults-from**
  Specifies the profile that you want to use as the parent profile. Your new profile inherits all settings and values from the parent profile specified. The default value is **ftp**.
- **description**
  User defined description.
- **glob**
  Displays the items that match the **glob** expression. See **help glob** for a description of **glob** expression syntax.
- **name**
  Specifies a unique name for the component. This option is required for the commands **create**, **delete**, and **modify**.
- **partition**
  Displays the administrative partition within which the component resides.
- **port**
  Specifies a service for the data channel port used for this FTP profile. The default port is **ftp-data**.
- **regex**
  Displays the items that match the regular expression. The regular expression must be preceded by an at sign (@[regular expression]) to indicate that the identifier is a regular expression. See **help regex** for a description of regular expression syntax.

- **security**
  Enables or disables secure FTP traffic for the BIG-IP® Application Security Manager. You can set the security option only if the system is licensed for the BIG-IP Application Security Manager. The default value is **disabled**.
- **to-folder**
  ftp profiles can be moved to any folder under **/Common**, but configuration depenedencies may restrict moving the profile out of **/Common**.
- **translate-extended**
  This option is **enabled** by default, and thus, automatically translates RFC2428 extended requests EPSV and EPRT to PASV and PORT when communicating with IPv4 servers.
- **inherit-parent-profile**
  Enables the FTP data channel to inherit the TCP profile used by the control channel. If **disabled**, the data channel uses FastL4 (BigProto) only.
- **log-publisher**
  Specify the name of the log publisher which logs translation events. See **help sys log-config** for more details on the logging sub-system. Use the *publisher* component to set up a log publisher.
- **log-profile**
  Specify the name of the ALG log profile which controls the logging of ALG . See **help ltm alg-log-profile** for more details on the logging profile sub-system. Use the ltm alg-log-profile profile component to set up a ALG log profile.

See Also

create, *delete*, *edit*, glob, *list*, *virtual*, *modify*, *mv*, regex, *reset-stats*, *show*, *tmsh*

html

Configures an HTML profile.

Syntax

Configure the **html** component within the **ltm profile** module using the syntax shown in the following sections.

Create/Modify

```
create html [name]
modify html [name]
    defaults-from [ [name] | none]
    content-detection [disabled | enabled]
    content-selection
      [add | delete | replace-all-with] {
        [content-type] ...
    }
    content-selection none
    rules
      [add | delete | replace-all-with] {
        [html-rule] ...
    }
    rules none
```

```
mv html [ [[source-name] [destination-name]] | [[name] to-folder [folder-name]] |
[[name...name] to-folder [folder-name]] ]
    to-folder
```

```
reset-stats html
reset-stats html [ [ [name] | [glob] | [regex] ] ... ]
```

Display

```
list html
list html [ [ [name] | [glob] | [regex] ] ... ]
show running-config html
show running-config html [ [ [name] | [glob] | [regex] ] ... ]
    all-properties
    non-default-properties
    one-line
    partition
```

```
show html
show html [ [ [name] | [glob] | [regex] ] ... ]
     (default | exa | gig | kil | meg | peta | raw | tera | yotta | zetta)
     field-fmt
     global
```

Delete

```
delete html [name]
```

Description

Use this command to create, modify, display, or delete an HTML profile with which you can manage HTML traffic.

Examples

create html my_html_profile defaults-from html

Creates a custom HTML profile named **my_html_profile** that inherits its settings from the system default HTML profile.

list html

Displays the properties of all HTML profiles.

mv html /Common/my_html_profile to-folder /Common/my_folder

Moves a custom HTML profile named **my_html_profile** to a folder named **my_folder**, where **my_folder** has already been created and exists within **/Common**.

Please refer to the mv manual page for examples on how to use the mv command.

Options

- **defaults-from**
  Specifies the profile that you want to use as the parent profile. Your new profile inherits all settings and values from the parent profile specified. The default value is **html**.
- **description**
  User defined description.
- **glob**
  Displays the items that match the **glob** expression. See **help glob** for a description of **glob** expression syntax.
- **name**
  Specifies a unique name for the component. This option is required for the commands **create**, **delete**, and **modify**.
- **partition**
  Displays the administrative partition within which the component resides.
- **content-detection**
  Scans initial HTTP payload to look for HTML signatures and enables HTML profile if HTML-like patterns are detected.
- **content-selection**
  Matches content-type from response header against a list of content-types and enables HTML profile if a match is found.
- **rules**
  Specifies a list of HTML (content rewrite) rules, separated by spaces, that are used for parsing and patching HTML.

- **to-folder**
  html profiles can be moved to any folder under **/Common**, but configuration depenedencies may restrict moving the profile out of **/Common**.

See Also

create, *delete*, glob, *list*, *virtual*, *modify*, *mv*, *reset-stats*, *show*, *tmsh*

http

Configures an HTTP profile.

Syntax

Configure the **http** component within the **ltm profile** module using the syntax shown in the following sections.

Create/Modify

```
create http [name]
modify http [name]
    accept-xff [disabled | enabled]
    app-service [[string] | none]
    basic-auth-realm [ ["string"] | none]
    defaults-from [ [name] | none]
    description [string]
    encrypt-cookie-secret [none | [passphrase] ]
    encrypt-cookies
      [add | delete | replace-all-with] {
        [cookie] ...
    }
    encrypt-cookies none
    enforcement {
        excess-client-headers [disabled | enabled]
        excess-server-headers [disabled | enabled]
        max-header-size [integer]
        max-header-count [integer]
        max-requests [integer]
        oversize-client-headers [disabled | enabled]
        oversize-server-headers [disabled | enabled]
        pipeline [allow | pass-through | reject]
        truncated-redirects [disabled | enabled]
        unknown-method [allow | pass-through | reject]
    }
    fallback-host [ [hostname] | none]
    fallback-status-codes
      [add | delete | replace-all-with] {
        [fallback status code]...
    }
    fallback-status-codes none
    header-erase [none | [string] ]
    header-insert [none | [string] ]
    insert-xforwarded-for [disabled | enabled]
    lws-separator [none | string ]
    lws-width [integer]
    oneconnect-transformations [disabled | enabled]
    proxy-type [reverse | explicit | transparent]
    redirect-rewrite [all | matching | nodes | none]
    request-chunking [preserve | rechunk | selective ]
    response-chunking [preserve | rechunk | selective | unchunk]
    response-headers-permitted
      [add | delete | replace-all-with] {
        [response header] ...
    }
    response-headers-permitted none
```

```
    server-agent-name [string]
    explicit-proxy {
        enabled [no | yes]
        dns-resolver [dns-resolver]
        tunnel-name [tunnel]
        route-domain [route-domain]
        default-connect-handling [deny | allow]
        connect-error-message ["string"]
        dns-error-message ["string"]
        bad-request-message ["string"]
        bad-response-message ["string"]
    }
    sflow {
        poll-interval [integer]
        poll-interval-global [no | yes]
        sampling-rate [integer]
        sampling-rate-global [no | yes]
    }
    via-host-name [string]
    via-request [append | preserve | remove]
    via-response [append | preserve | remove]
    xff-alternative-names
      [add | delete | replace-all-with] {
        [xff alternative name] ...
    }
edit http [ [ [name] | [glob] | [regex] ] ... ]
    all-properties
    non-default-properties
mv http [ [[source-name] [destination-name]] | [[name] to-folder [folder-name]] |
[[name...name] to-folder [folder-name]] ]
    to-folder
reset-stats http
reset-stats http [ [ [name] | [glob] | [regex] ] ... ]
```

Display

```
list http
list http [ [ [name] | [glob] | [regex] ] ... ]
show running-config http
show running-config http [ [ [name] | [glob] | [regex] ] ... ]
    all-properties
    non-default-properties
    one-line
    partition
show http
show http [ [ [name] | [glob] | [regex] ] ... ]
     (default | exa | gig | kil | meg | peta | raw | tera | yotta | zetta)
     field-fmt
     global
```

Delete

```
delete http [name]
```

Description

You can use the **http** component to create, modify, display, or delete an HTTP profile.

The BIG-IP® system installation includes the following default HTTP-type profiles:

- **http**

The default HTTP profile contains values for properties related to managing HTTP traffic.

You can create a new HTTP-type profile using an existing profile as a parent profile, and then you can change the values of the properties to suit your needs.

Examples

create http my_http_profile defaults-from http

Creates a custom HTTP profile named **my_http_profile** that inherits its settings from the system default HTTP profile.

mv http /Common/my_http_profile to-folder /Common/my_folder

Moves a custom HTTP profile named **my_http_profile** to a folder named **my_folder**, where **my_folder** has already been created and exists within **/Common**.

Please refer to the mv manual page for examples on how to use the mv command.

Options

- **accept-xff**
  Enables or disables trusting the client IP address, and statistics from the client IP address, based on the request's XFF (X-forwarded-for) headers, if they exist.
- **app-service**
  Specifies the name of the application service to which the profile belongs. The default value is **none**. **Note:** If the **strict-updates** option is **enabled** on the application service that owns the object, you cannot modify or delete the profile. Only the application service can modify or delete the profile.
- **basic-auth-realm**
  Specifies a quoted string for the basic authentication realm. The system sends this string to a client whenever authorization fails. The default value is **none**.

- **defaults-from**
  Specifies the profile that you want to use as the parent profile. Your new profile inherits all settings and values from the parent profile specified. The default value is **http**.
- **description**
  User defined description.
- **encrypt-cookie-secret**
  Specifies a passphrase for the cookie encryption. The default value is **none**.
- **encrypt-cookies**
  Specifies to encrypt specific cookies that the BIG-IP system sends to a client system. The default value is **none**.
- **enforcement**
  Specifies protocol enforcement options for the HTTP proile:
  - **excess-client-headers**
    Specifies the pass-through behavior when **max-header-count** is exceeded by the client. The default is **disabled** which rejects the connection.
  - **excess-server-headers**
    Specifies the pass-through behavior when **max-header-count** is exceeded by the server. The default is **disabled** which rejects the connection.
  - **known-methods**
    Specifies the HTTP methods known by the HTTP filter. Combine with the **unknown-method** field to control behavior when unusual methods are parsed.
  - **max-header-size**
    Specifies the maximum header size. The default value is **32768**.
  - **max-header-count**
    Specifies the maximum number of headers in HTTP request or response that will be handled. If client or server sends request or response with the number of headers greater then specified, the connection will be dropped. The default value is 64.
  - **max-requests**
    Specifies the number of requests that the system accepts on a per-connection basis. The default value is **0** (zero), which means the system does not limit the number of requests per connection.
  - **oversize-client-headers**
    Specifies the pass-through behavior when **max-header-size** is exceeded by the client. The default is **disabled** which rejects the connection.
  - **oversize-server-headers**
    Specifies the pass-through behavior when **max-header-size** is exceeded by the server. The default is **disabled** which rejects the connection.

- **pipeline**
  Enables or disables HTTP/1.1 pipelining. If **pass-through** is chosen, then the HTTP filter will switch to pass through mode (and be disabled) if pipelined data is seen. The default value is **allow**, which means that clients can make requests even when prior requests have not received a response. In order for this to succeed, however, destination servers must include support for pipelining.
- **to-folder**
  http profiles can be moved to any folder under **/Common**, but configuration depenedencies may restrict moving the profile out of **/Common**.
- **truncated-redirects**
  Specifies the pass-through behavior when a redirect lacking the trailing carriage-return and line feed pair at the end of the headers is parsed. The default is **disabled**, which will silently drop the invalid HTTP.
- **unknown-method**
  Specifies the behavior (**allow**, **reject**, or **pass-through**) when an unknown HTTP method is parsed. The default is to **allow** unknown methods.

◆ **fallback-host**
Specifies an HTTP fallback host. The default value is **none**.
With HTTP redirection, you can redirect HTTP traffic to another protocol identifier, host name, port number, or URI path. For example, if all members of a targeted pool are unavailable (that is, the members are disabled, marked as **down**, or have exceeded their connection limit), the system can redirect the HTTP request to the fallback host, with the HTTP reply Status Code 302 Found.

◆ **fallback-status-codes**
Specifies one or more three-digit status codes that can be returned by an HTTP server. The default value is **none**.

◆ **glob**
Displays the items that match the **glob** expression. See **help glob** for a description of **glob** expression syntax.

◆ **header-erase**
Specifies the header string that you want to erase from an HTTP request. The default value is **none**.

◆ **header-insert**
Specifies a quoted header string that you want to insert into an HTTP request. The default value is **none**.
The HTTP header being inserted can include a client IP address. Including a client IP address in an HTTP header is useful when a connection goes through a secure network address translation (SNAT) and you need to preserve the original client IP address. When you assign the configured HTTP profile to a virtual server, the system then inserts the header specified by the profile into any HTTP request that the system sends to a pool or pool member.

- **insert-xforwarded-for**
  Enables or disables insertion of an X-Forwarded-For header. The default value is **disabled**.
  When using connection pooling, which allows clients to make use of other client requests' server connections, you can insert the X-Forwarded-For header and specify a client IP address.
- **lws-separator**
  Specifies the linear white space separator that the system uses between HTTP headers when a header exceeds the maximum width specified in the **lws-width** option. The valid value should be none, or, any combination of cr(carriage return), lf(line feed), or sp(space). The default value is **none**.
- **lws-width**
  Specifies the maximum number of columns that a header that is inserted into an HTTP request can have. The default value is **80**.
- **name**
  Specifies a unique name for the component. This option is required for the commands **create**, **delete**, and **modify**.
- **oneconnect-transformations**
  Specifies whether the system performs HTTP header transformations for the purpose of keeping server-side connections open. The default value is **enabled**. This feature requires configuration of a OneConnect™ profile.
- **partition**
  Displays the partition within which the component resides.
- **redirect-rewrite**
  Specifies which of the application HTTP redirects the system rewrites to HTTPS. The options are:
  - **all**
    Specifies to rewrite all application redirects to HTTPS.
  - **matching**
    Specifies to rewrite to HTTPS only application redirects that match the original URI exactly.
  - **nodes**
    If the URI contains a node IP address, instead of a host name, specifies that the system rewrites the node IP address to the virtual server IP address.
  - **none**
    Specifies that the system does not rewrite to HTTPS any application HTTP redirects. This is the default value.

  Use this feature when an application is generating HTTP redirects that send the client to HTTP (a non-secure channel) when you want the client to continue accessing the application using HTTPS (a secure channel). This is a common occurrence when using client SSL processing on a BIG-IP system.

- **regex**
  Displays the items that match the regular expression. The regular expression must be preceded by an at sign (@[regular expression]) to indicate that the identifier is a regular expression. See **help regex** for a description of regular expression syntax.
- **request-chunking**
  Specifies how to handle chunked and unchunked requests. The default value is **selective**. The options are described under **response-chunking**.
- **response-chunking**
  Specifies how to handle chunked and unchunked responses. The default value is **selective**. The options are:
  - **unchunk**
    If the request or response is chunked, this option unchunks the request or response, processes the HTTP content, and passes the request or response on as unchunked. The Keep-Alive value for the Connection header is not supported, and therefore the system sets the value of the header to close.
    If the request or response is unchunked, the LTM system processes the HTTP content and passes the request or response on untouched.
  - **rechunk**
    If the request or response is chunked, the system unchunks the request or response, processes the HTTP content, re-adds the chunk trailer headers, and then passes on the request or response as chunked. Any chunk extensions are lost.
    If the request or response is unchunked, the system adds transfer encoding and chunking headers on egress.
  - **preserve**
    If the request or response is chunked or unchunked, the system leaves the request or response chunked, processes the HTTP content, and passes the request or response on untouched.
  - **selective**
    If the request or response is chunked, the system unchunks the request or response, processes the HTTP content, re-adds the chunk trailer headers, and then passes on the request or response as chunked. Any chunk extensions are lost.
    If the request is unchunked, the system processes the HTTP content, and then passes on the request or response untouched.
- **response-headers-permitted**
  Specifies headers that the BIG-IP system allows in an HTTP response. The default value is **none**.
- **explicit-proxy**
  Specifies explicit settings for the HTTP profile:
  - **enabled**
    Specifies whether the explicit proxy service is enabled or disabled. The default it is **no**.
  - **dns-resolver**
    Specifies the dns-resolver object that will be used to resolve hostnames in proxy requests. The default is **dns-resolver**.

- **tunnel-name**
  Specifies the tunnel that will be used for outbound proxy requests. This enables other virtual servers to receive connections initiated by the proxy service. The default is **http-tunnel**.
- **route-domain**
  Specifies the route-domain that will be used for outbound proxy requests. The default is **0**.
- **default-connect-handling**
  Specifies the behavior of the proxy service for CONNECT requests. If set to **deny**, CONNECT requests will only be honored if there is another virtual server listening for the requested outbound connection. If set to **allow** outbound connections will be made regardless of other virtual servers. The default is **deny**.
- **host-names**
  Specifies the which host names are to be treated as local. Proxy requests made for those hosts will be treated as regular HTTP requests and will be sent to the configured default pool.
- **connect-error-message**
  Specifies the error message that will be returned to the browser when a proxy request can't be completed because of a failure to establish the outbound connection.
- **dns-error-message**
  Specifies the error message that will be returned to the browser when a proxy request can't be completed because of a failure to resolve the hostname in the request.
- **bad-request-message**
  Specifies the error message that will be returned to the browser when a proxy request can't be completed because the request was malformed.
- **bad-response-message**
  Specifies the error message that will be returned to the browser when a proxy request can't be completed because the response was malformed.

◆ **sflow**
Specifies sFlow settings for the HTTP profile:

- **poll-interval**
  Specifies the maximum interval in seconds between two pollings. The default value is **0**. To enable this setting, you must also set the **poll-interval-global** setting to **no**.
- **poll-interval-global**
  Specifies whether the global HTTP poll-interval setting, which is available under **sys sflow global-settings** module, overrides the object-level poll-interval setting. The default value is **yes**.
  The available values are:
  - **no**
    Specifies to use the object-level poll-interval setting.

- **yes**
  Specifies to use the global HTTP poll-interval setting.

- **sampling-rate**
  Specifies the ratio of packets observed to the samples generated. For example, a sampling rate of 2000 specifies that 1 sample will be randomly generated for every 2000 packets observed. The default value is **0**. To enable this setting, you must also set the **sampling-rate-global** setting to **no**.

- **sampling-rate-global**
  Specifies whether the global HTTP sampling-rate setting, which is available under **sys sflow global-settings** module, overrides the object-level sampling-rate setting. The default value is **yes**.
  The available values are:

  - **no**
    Specifies to use the object-level sampling-rate setting.

  - **yes**
    Specifies to use the global HTTP sampling-rate setting.

◆ **via-host-name**
Specifies the hostname that will be used in the **Via:** HTTP header. See **via-request** and **via-response** for how the **Via:** header will be handled. If either **via-request** or **via-response** are set to **append**, then this is required.

◆ **via-request**
Specifies how you want to process **Via:** HTTP header in requests sent to OWS. The default setting is **remove**. The available values are:

- **append**
  The value from **via-host-name** is appended to the **Via:** HTTP header.

- **preserve**
  Via: HTTP header is preserved without changes.

- **remove**
  Via: HTTP header is removed from the request.

-

◆ **via-response**
Specifies how you want to process **Via:** HTTP header in responses sent to clients. The default setting is **remove**. The available values are the same as in **via-request**.

◆ **server-agent-name**
Specifies the string used as the server name in traffic generated by LTM. The default value is **BigIP**.

◆ **alternative-xff-names**
Specifies alternative XFF headers instead of the default X-forwarded-for header.

See Also

create, *delete*, *edit*, glob, *list*, *fasthttp*, *virtual*, *modify*, *mv*, regex, *reset-stats*, *show*, *tmsh*

http-compression

Configures an HTTP Compression profile.

Syntax

Configure the **http-compression** component within the **ltm profile** module using the syntax shown in the following sections.

Create/Modify

```
create http-compression [name]
modify http-compression [name]
    allow-http-10 [disabled | enabled]
    app-service [[string] | none]
    browser-workarounds [disabled | enabled]
    buffer-size [integer]
    cpu-saver [disabled | enabled]
    cpu-saver-high [integer]
    cpu-saver-low [integer]
    content-type-exclude
      [add | delete | replace-all-with] {
        [content type] ...
    }
    content-type-exclude none
    content-type-include
      [add | delete | replace-all-with] {
        [content type] ...
    }
    content-type-include none
    defaults-from [ [name] | none]
    description [string]
    gzip-level [integer]
    gzip-memory-level [integer, in bytes]
    gzip-window-size [integer]
    keep-accept-encoding [disabled | enabled]
    method-prefer [deflate | gzip]
    min-size [integer]
    selective [disabled | enabled]
    uri-exclude
      [add | delete | replace-all-with] {
        [URI] ...
    }
    uri-exclude none
    uri-include
      [add | delete | replace-all-with] {
        [URI] ...
    }
    uri-include none
    vary-header [disabled | enabled]
edit http-compression [ [ [name] | [glob] | [regex] ] ... ]
    all-properties
    non-default-properties
mv http-compression [ [[source-name] [destination-name]] | [[name] to-folder
[folder-name]] | [[name...name] to-folder [folder-name]] ]
    to-folder
```

```
reset-stats http-compression
reset-stats http-compression [ [ [name] | [glob] | [regex] ] ... ]
```

Display

```
list http-compression
list http-compression [ [ [name] | [glob] | [regex] ] ... ]
show running-config http-compression
show running-config http-compression [ [ [name] | [glob] | [regex] ]
                                       ... ]
    all-properties
    non-default-properties
    one-line
    partition
show http-compression
show http-compression [ [ [name] | [glob] | [regex] ] ... ]
     (default | exa | gig | kil | meg | peta | raw | tera | yotta | zetta)
     field-fmt
     global
```

Delete

```
delete http-compression [name]
```

Description

You can use the **http-compression** component to create, modify, display, or delete an HTTP Compression profile.

The BIG-IP® system installation includes the following default HTTP Compression-type profiles:

- **http-compression**
- **wan-optimized-compression**

The default HTTP Compression profile contains values for properties related to managing compression settings.

You can create a new HTTP Compression-type profile using an existing profile as a parent profile, and then you can change the values of the properties to suit your needs.

Examples

create http-compression my_hc_profile defaults-from http-compression

Creates a custom HTTP Compression profile named **my_hc_profile** that inherits its settings from the system default HTTP Compression profile.

mv http-compression /Common/my_httpcompression_profile to-folder /Common/my_folder

Moves a custom http-compression profile named **my_httpcompression_profile** to a folder named **my_folder**, where **my_folder** has already been created and exists within **/Common**.

Options

- **allow-http10**
  Enables or disables compression of HTTP/1.0 server responses. The default value is **disabled**.
- **app-service**
  Specifies the name of the application service to which the profile belongs. The default value is **none**. **Note:** If the **strict-updates** option is **enabled** on the application service that owns the object, you cannot modify or delete the profile. Only the application service can modify or delete the profile.
- **browser-workarounds**
  Enables or disables compression of browser workarounds. The default value is **disabled**. Enabling this options turns off compression on server responses when any of the following conditions are detected:
  - If the client browser is Netscape Navigator® version 4.0x, compression is turned off. Netscape advertises that the browser can handle compression gracefully. In this case, F5 Networks disables compression entirely for that class of browser.
  - If the client browser is Netscape Navigator version 4.x (4.10 and later) and the server response Content-Type is not either text/html or text/plain compression is turned off. This class of Netscape browsers can handle plain text and HTML just fine, but there are known issues with other types of content.
  - If the client browser is Microsoft® Internet Explorer (any version), the server response Content-Type is either text/css or application/x-javascript, and the client connection is over SSL, compression is turned off. The Microsoft article ID for this problem is 825057.
  - If the client browser is Microsoft Internet Explorer (any version), the server response Content-Type is either text/css or application/x-javascript, and the server sets the header Cache-Control to no-cache, compression is turned off. The Microsoft article ID for this problem is 327286.
- **buffer-size**
  Specifies the maximum number of uncompressed bytes that the system buffers before determining whether to compress the response. Useful when the headers of a server response do not specify the length of the response content. The default value is **4096**.

- **content-type-exclude**
  Specifies a string list of HTTP Content-Type responses that you do not want the system to compress. The default value is **none**.
- **content-type-include**
  Specifies a string list of HTTP Content-Type responses that you want the system to compress. The default value is **{ text/ application/ (xml|x-javascript) }**.
- **cpu-saver**
  Enables or disables the CPU saver feature. When the CPU saver is **enabled**, the system monitors the percent of CPU usage and adjusts compression rates automatically when the CPU usage reaches the percentage defined in the **compress-cpu-saver-low** and **compress-cpu-saver-high** options. The default value is **enabled**.
- **cpu-saver-high**
  Specifies the percent of CPU usage at which the system starts automatically decreasing the amount of content being compressed, as well as the amount of compression that the system is applying. The default value is **90**.
- **cpu-saver-low**
  Specifies the percent of CPU usage at which the system resumes content compression at the user-defined rates. The default value is **75**.
- **defaults-from**
  Specifies the profile that you want to use as the parent profile. Your new profile inherits all settings and values from the parent profile specified. The default value is **httpcompression**.
- **description**
  User defined description.
- **gzip-level**
  Specifies a value that determines the amount of memory that the system uses when compressing a server response. The default value is **1**.
- **gzip-memory-level**
  Specifies the amount of memory (in kilobytes) that the system uses when compressing a server response. The system rounds the value up to the nearest power of two. The default value is **8**. The maximum value is **256**.
- **gzip-window-size**
  Specifies the number of kilobytes in the window size that the system uses when compressing a server response. The system rounds the value up to the nearest power of two. The default value is **16k**. The maximum value is **128k**.
- **keep-accept-encoding**
  Specifies where data compression is performed. When **enabled**, the target server, rather than the BIG-IP local traffic management system, performs data compression. The default value is **disabled**.
- **method-prefer**
  Specifies the type of compression that the system prefers. The default value is **gzip**.

- **min-size**
  Specifies the minimum length in bytes of a server response that is acceptable for compression. The length in bytes applies to content length only, not headers. The default value is **1024**.
- **partition**
  Displays the administrative partition within which the profile resides.
- **selective**
  Enables or disables selective compression mode. Note that the data compression feature compresses HTTP server responses, and not client requests. The default value is **disabled**.
- **to-folder**
  http-compression profiles can be moved to any folder under **/Common**, but configuration depenedencies may restrict moving the profile out of **/Common**.
- **uri-exclude**
  Disables compression on a specified list of HTTP Request-URI responses. Use a regular expression to specify a list of URIs you do not want to compress. The default value is **none**.
- **uri-include**
  Enables compression on a specified list of HTTP Request-URI responses. Use a regular expression to specify a list of URIs you want to compress. The default value is **none**.
- **vary-header**
  Enables or disables the insertion of a Vary header into cacheable server responses. The default value is **enabled**.

See Also

create, *delete*, *edit*, glob, *list*, *fasthttp*, *virtual*, *modify*, *mv*, regex, *reset-stats*, *show*, *tmsh*

http2

Configures a HTTP/2 protocol profile.

Syntax

Configure the **http2** component within the **ltm profile** module using the syntax shown in the following sections.

Create/Modify

```
create http2 [name]
modify http2 [name]
    activation-modes { [npn | alpn | always] ... }
    concurrent-streams-per-connection [integer]
    connection-idle-timeout [integer]
    defaults-from [ [name] | none]
    description [string]
    frame-size [integer]
    insert-header [disabled | enabled]
    insert-header-name ["string"]
    receive-window [integer]
    write-size [integer]
    header-table-size [integer]
```

Display

```
list http2
list http2 [ [ [name] | [glob] | [regex] ] ... ]
show running-config http2
show running-config http2 [ [ [name] | [glob] | [regex] ] ... ]
    all-properties
    non-default-properties
    one-line
    partition
show http2
show http2 [ [ [name] | [glob] | [regex] ] ... ]
    (default | exa | gig | kil | meg | peta | raw | tera | yotta | zetta)
    field-fmt
    global
```

Delete

```
delete http2 [name]
```

Description

You can use the **http2** component to create, modify, display, or delete a HTTP/2 profile.

The BIG-IP® system installation includes the following default HTTP/2-type profiles:

- **http2**

The default HTTP/2 profile contains values for properties related to managing HTTP/2 traffic.

You can create a new HTTP/2-type profile using an existing profile as a parent profile, and then you can change the values of the properties to suit your needs.

Examples

create http2 my_http2_profile defaults-from http2

Options

- **activation-modes**
  Specifies what will cause a connection to be treated as a HTTP/2 connection. The values **npn** and **alpn** specify that the TLS next-protocol-negotiation and application-layer-protocol-negotiation will be used to determine whether HTTP/2 should be activated. Clients that use TLS, but only support HTTP will work as-if HTTP/2 is not present. The value **always** specifies that all connections are assumed to be HTTP/2 connections. The default value is **{ npn alpn }**.
- **concurrent-streams-per-connection**
  Specifies how many concurrent requests are allowed to be outstanding on a single HTTP/2 connection.
- **connection-idle-timeout**
  Specifies how many seconds a HTTP/2 connection is left open idly before it is shutdown.
- **defaults-from**
  Specifies the profile that you want to use as the parent profile. Your new profile inherits all settings and values from the parent profile specified. The default value is **http2**.
- **description**
  User defined description.
- **frame-size**
  Specifies the size of the data frames, in bytes, that HTTP/2 will send to the client. Larger frame sizes will improve network utilization, but may affect concurrency. The default value is **2048**.
- **glob**
  Displays the items that match the **glob** expression. See **help glob** for a description of **glob** expression syntax.
- **insert-header**
  Specifies whether an HTTP header that indicates the use of HTTP/2 should be inserted in the request going to the back-end server. The default value is **disabled**.

- **insert-header-name**
  Specifies the name of the HTTP header controlled by **insert-header**. The default value is **"X-HTTP/2"**.
- **name**
  Specifies a unique name for the component. This option is required for the commands **create**, **delete**, and **modify**.
- **receive-window**
  Specifies the receive window, in KB. The receive window is a mechanism used by HTTP/2 to perform flow control. The receive window allows HTTP/2 to stall individual upload streams when needed. This mechanism is available only for HTTP/2 version 3. The default value is **32**.
- **regex**
  Displays the items that match the regular expression. The regular expression must be preceded by an at sign (@[regular expression]) to indicate that the identifier is a regular expression. See **help regex** for a description of regular expression syntax.
- **write-size**
  Specifies the total size of combined data frames, in bytes, HTTP/2 will send in a single write. This controls the size of the TLS records when HTTP/2 is used over SSL. A large write size will cause HTTP/2 to buffer more data, but will improve network utilization. The default value is **16384**.
- **header-table-size**
  Specifies the size of the header table, in KB. The HTTP/2 protocol compresses http headers to save bandwidth. A larger table will allow better compression, at the cost of more memory usage. The default value is **4**. This is currently unused.

See Also

create, *delete*, *edit*, glob, *list*, *fasthttp*, *virtual*, *modify*, regex, *reset-stats*, *show*, *tmsh*

icap

Configures an Internet Content Adaptation Protocol (ICAP) profile.

Syntax

Configure the **icap** component within the **ltm profile** module using the syntax shown in the following sections.

Create/Modify

```
create icap [name]
modify icap [name]
    defaults-from [ [name] | none]
    description [string]
    header-from [string]
    host [string]
    preview-length [integer]
    referer [string]
    uri [string]
    user-agent [string]
edit icap [ [ [name] | [glob] | [regex] ] ... ]
    all-properties
    non-default-properties
mv icap [ [[source-name] [destination-name]] | [[name] to-folder [folder-name]] |
[[name...name] to-folder [folder-name]] ]
    to-folder
reset-stats icap
reset-stats icap [ [ [name] | [glob] | [regex] ] ... ]
```

Display

```
list icap
list icap [ [ [name] | [glob] | [regex] ] ... ]
show running-config icap
show running-config icap [ [ [name] | [glob] | [regex] ] ... ]
    all-properties
    non-default-properties
    one-line
    partition
show icap
show icap [ [ [name] | [glob] | [regex] ] ... ]
    (default | exa | gig | kil | meg | peta | raw | tera | yotta | zetta)
    field-fmt
```

Delete

```
delete icap [name]
```

Description

You can use the **icap** component to manage an Internet Content Adaptation Protocol profile.

Examples

create icap my_icap defaults-from icap

Creates an internet content adaptation protocol profile named **my_icap** using the system defaults.

create icap my_icap { uri icap://mycompany.com/ad_insertion/ }

Creates an internet content adaptation protocol profile named **my_icap** that uses **icap://mycompany.com/ad_insertion/** as the ICAP URI.

mv icap /Common/my_icap_profile to-folder /Common/my_folder

Moves a custom icap profile named **my_icap_profile** to a folder named **my_folder**, where **my_folder** has already been created and exists within **/Common**.

- **defaults-from**
  Specifies the profile that you want to use as the parent profile. Your new profile inherits all of the settings and values from the specified parent profile. The default value is **icap**.
- **description**
  User defined description.
- **header-from**
  Specifies the header-from attribute to use in the ICAP header. Please refer to RFC 3507 section 4.3.2.
- **host**
  Specifies the host attribute to use the in the ICAP header. Please refer to RFC 3507 section 4.3.2i.
- **preview-length**
  Specifies the ICAP data preview size. Please refer to RFC 3507 section 4.5.
- **referer**
  Specifies the referer attribute to use in the ICAP header. Please refer to RFC 3507 section 4.3.2.
- **to-folder**
  icap profiles can be moved to any folder under **/Common**, but configuration dependencies may restrict moving the profile out of **/Common**.
- **uri**
  Specifies the ICAP URI to use in the ICAP header. Please refer to RFC 3507 section 4.2. Macro expansion has been implemented for all attributes values in the ICAP header. If an ICAP header attribute value contains **${SERVER_IP}**, the macro will be replaced with the IP address of the ICAP server selected from the internal virtual server's pool. If an ICAP header attribute contains **${SERVER_PORT}**, the macro will be

replaced with the port of the ICAP server selected from the internal virtual server's pool. For example, the URI attribute in an ICAP profile could be set to **icap://${SERVER_IP}:${SERVER_PORT}/videoOptimization**.

- **user-agent**
  Specifies the user-agent attribute to use in the ICAP header. Please refer to RFC 3507 section 4.3.2.

See Also

create, *delete*, *edit*, glob, *list*, *virtual*, *modify*, *mv*, regex, *reset-stats*, *show*, *tmsh*, *response-adapt*

iiop

Configures an Internet Inter-Orb Protocol (IIOP) profile.

Syntax

Configure the **iiop** component within the **ltm profile** module using the syntax shown in the following sections.

Create/Modify

```
create iiop [name]
modify iiop [name]
    abort-on-timeout [disabled | enabled]
    app-service [[string] | none]
    defaults-from [name]
    description [string]
    persist-object-key [disabled | enabled]
    persist-request-id [disabled | enabled]
    timeout [integer]
edit iiop [ [ [name] | [glob] | [regex] ] ... ]
    all-properties
    non-default-properties
reset-stats iiop
reset-stats iiop [name]
```

Display

```
list iiop
list iiop  [ [ [name] | [glob] | [regex] ] ... ]
show running-config iiop
show running-config iiop  [ [ [name] | [glob] | [regex] ] ... ]
    all-properties
    non-default-properties
    one-line
    partition
show iiop
show iiop  [ [ [name] | [glob] | [regex] ] ... ]
    (default | exa | gig | kil | meg | peta | raw | tera | yotta | zetta)
    field-fmt
    global
```

Delete

```
delete iiop [name]
```

Description

You can use the **iiop** component to manage IIOP network traffic. The system parses the incoming TCP stream, disaggregates it into IIOP messages, and performs load balancing and persistence based on the parameters you set.

Examples

create iiop my_iiop_profile defaults-from iiop

Creates an IIOP profile named **my_iiop_profile** that inherits its settings from the system default IIOP profile named **iiop**.

list iiop all-properties

Displays all properties for all IIOP profiles.

Options

- **abort-on-timeout**
  Specifies whether the system aborts the connection if there is no response received within the time specified in the **timeout** option. The default value is **disabled**.
- **app-service**
  Specifies the name of the application service to which the profile belongs. The default value is **none**. **Note:** If the **strict-updates** option is **enabled** on the application service that owns the object, you cannot modify or delete the profile. Only the application service can modify or delete the profile.
- **defaults-from**
  Specifies the profile that you want to use as the parent profile. Your new profile inherits all settings and values from the parent profile specified. The default value is **iiop**.
- **description**
  User defined description.
- **glob**
  Displays the items that match the **glob** expression. See **help glob** for a description of **glob** expression syntax.
- **name**
  Specifies a unique name for the component. This option is required for the commands **create**, **delete**, and **modify**.
- **partition**
  Displays the administrative partition within which this profile resides.
- **persist-object-key**
  Specifies whether to persist connections based on the object key in the IIOP request. The default value is **disabled**.
- **persist-request-id**
  Specifies whether to persist connections based on the request ID in the IIOP request. The default value is **enabled**.
- **regex**
  Displays the items that match the regular expression. The regular expression must be preceded by an at sign (@[regular expression]) to indicate that the identifier is a regular expression. See **help regex** for a description of regular expression syntax.

- **timeout**
  Specifies the request timeout. The system uses this value when the **abort-on-timeout** option is **enabled**. The default value is **30** seconds.

See Also

create, *delete*, *edit*, glob, *list*, *virtual*, *modify*, regex, *reset-stats*, *show*, *tmsh*

ipother

Configures a generic IP profile for non-TCP and non-UDP traffic.

Syntax

Configure the **ipother** component within the **ltm profile** module using the syntax shown in the following sections.

Create/Modify

```
create ipother [name]
modify ipother [name]
    app-service [[string] | none]
    defaults-from [[name] | none]
    description [string]
    idle-timeout [immediate | indefinite | integer]
edit ipother [ [ [name] | [glob] | [regex] ] ... ]
    all-properties
    non-default-properties
reset-stats ipother
reset-stats ipother [ [ [name] | [glob] | [regex] ] ... ]
```

Display

```
list ipother
list ipother [ [ [name] | [glob] | [regex] ] ... ]
show running-config ipother
show running-config ipother
  [ [ [name] | [glob] | [regex] ] ... ]
    all-properties
    non-default-properties
    one-line
    partition
show ipother
show ipother [ [ [name] | [glob] | [regex] ] ... ]
    (default | exa | gig | kil | meg | peta | raw | tera | yotta | zetta)
    field-fmt
    global
```

Delete

```
delete ipother [name]
```

Description

You can use the **ipother** component to manage non-TCP and non-UDP network traffic. If you want to manage TCP or UDP traffic, then use the approprite TCP or UDP LTM profiles.

Examples

create ipother my_ipother_profile defaults-from ipother

This creates a custom IP-OTHER profile that is named **my_ipother_profile** which inherits its settings from the system default IP-OTHER profile.

list ipother all-properties

Displays all properties for all IP-OTHER profiles.

Options

- **app-service**
  Specifies the name of the application service to which the profile belongs. The default value is **none**. **Note:** If the **strict-updates** option is **enabled** on the application service that owns the object, you cannot modify or delete the profile. Only the application service can modify or delete the profile.
- **defaults-from**
  Specifies the profile that you want to use as the parent profile. Your new profile inherits all settings and values from the parent profile. The default value is **ipother**.
- **description**
  User defined description.
- **glob**
  Displays the items that match the **glob** expression. See **help glob** for a description of **glob** expression syntax.
- **idle-timeout**
  Specifies the number of seconds that a connection is idle before the connection is eligible for deletion. The default value is **60** seconds.
- **name**
  Specifies a unique name for the component. This option is required for the commands **create**, **delete**, and **modify**.
- **partition**
  Displays the administrative partition within which the profile resides.
- **regex**
  Displays the items that match the regular expression. The regular expression must be preceded by an at sign (@[regular expression]) to indicate that the identifier is a regular expression. See **help regex** for a description of regular expression syntax.

See Also

create, *delete*, *edit*, glob, *ltm profile*, *virtual*, *modify*, *show*, regex, *reset-stats*, *tmsh*

mblb

Configures an MBLB profile (experimental).

Syntax

Configure the **mblb** component within the **ltm profile** module using the syntax shown in the following sections.

Create/Modify

```
create mblb [name]
modify mblb [name]
    app-service [[string] | none]
    defaults-from [ [name] | none]
    description [string]
    isolate-abort [disabled | enabled]
    isolate-expire [disabled | enabled]
    isolate-server [disabled | enabled]
    isolate-client [disabled | enabled]
    egress-high [# of messages]
    egress-low [# of messages]
    ingress-high [# of messages]
    ingress-low [# of messages]
    min-conn [# of connections]
    tag-ttl [# of seconds]
    shutdown-timeout [# of seconds]
edit mblb [ [ [name] | [glob] | [regex] ] ... ]
    all-properties
    non-default-properties
```

Display

```
list mblb
list mblb [ [ [name] | [glob] | [regex] ] ... ]
show running-config mblb
show running-config mblb [ [ [name] | [glob] | [regex] ] ... ]
    all-properties
    non-default-properties
```

Delete

```
delete mblb [name]
```

Description

Use this command to create, modify, display, or delete an MBLB profile with which you can customize MBLB behavior.

Examples

create mblb my_mblb_profile defaults-from mblb

Creates a custom MBLB profile named **my_mblb_profile** that inherits its settings from the system default MBLB profile.

list mblb

Displays the properties of all MBLB profiles.

Options

- **app-service**
  Specifies the name of the application service to which the profile belongs. The default value is **none**. **Note:** If the **strict-updates** option is **enabled** on the application service that owns the object, you cannot modify or delete the profile. Only the application service can modify or delete the profile.
- **defaults-from**
  Specifies the profile that you want to use as the parent profile. Your new profile inherits all settings and values from the parent profile specified. The default value is **mblb**.
- **description**
  User defined description.
- **glob**
  Displays the items that match the **glob** expression. See **help glob** for a description of **glob** expression syntax.
- **name**
  Specifies a unique name for the component. This option is required for the commands **create**, **delete**, and **modify**.
- **regex**
  Displays the items that match the regular expression. The regular expression must be preceded by an at sign (@[regular expression]) to indicate that the identifier is a regular expression. See **help regex** for a description of regular expression syntax.
- **isolate-abort**
  Specify whether to isolate abort event propagation.
- **isolate-expire**
  Specify whether to isolate expiration event propagation.
- **isolate-server**
  Specify whether to isolate serverside shutdown event propagation. This also dominate serverside abort/expiration event propagation.
- **isolate-client**
  Specify whether to isolate clientside shutdown event propagation. This also dominate clientside abort/expiration event propagation.
- **egress-high**
  Specify the high water mark for egress message queue. The default value is 50.

- **egress-low**
  Specify the low water mark for egress message queue. The default value is 5.
- **ingress-high**
  Specify the high water mark for ingress message queue. The default value is 50.
- **ingress-low**
  Specify the low water mark for ingress message queue. The default value is 5.
- **min-conn**
  Specify the minimum number of serverside connections. The default value is 0.
- **tag-ttl**
  Specify the TTL (time to live) for message TAG. The default value is 60.
- **shutdown-timeout**
  Delays sending FIN when BIGIP receives the first FIN packet from either the client or the server. Value of 0 means send FIN immediately otherwise the minimum of tcp idle timeout and shutdown timeout is used. The default value is 5 seconds

See Also

create, *delete*, *edit*, glob, *list*, *virtual*, *modify*, regex, *reset-stats*, *show*, *provision*, *tmsh*

mssql

Configures a profile to manage mssql(tds) database traffic.

Syntax

Configure the **mssql** component within the **ltm profile** module using the syntax in the following sections.

Create/Modify

```
create mssql [name]
modify mssql [name]
    read-pool [string]
    read-write-split-by-user [disabled | enabled]
    read-write-split-by-command [disabled | enabled]
    user-can-write-by-default [true | false]
    user-list  [add | delete | none | replace-all-with] {
            [user names...]
    }
    write-persist-timer [number]
    write-pool [string]
edit mssql [ [ [name] | [glob] | [regex] ] ... ]
    all-properties
    non-default-properties
reset-stats mssql
reset-stats mssql [ [ [name] | [glob] | [regex] ] ... ]
```

Display

```
list mssql
list mssql [ [ [name] | [glob] | [regex] ] ... ]
show running-config mssql
show running-config mssql [ [ [name] | [glob] | [regex] ] ... ]
    all-properties
    non-default-properties
    one-line
    partition
show mssql
show mssql [ [ [name] | [glob] | [regex] ] ... ]
    (default | exa | gig | kil | meg | peta | raw | tera | yotta | zetta)
    field-fmt
    global
```

Delete

```
delete mssql [name]
```

Description

You can use the **mssql** component to configure a profile to manage mssql(tds) database traffic.

Examples

create mssql my_mssql_profile defaults-from mssql

Creates a mssql profile named **my_mssql_profile** that inherits its settings from the system default mssql profile.

list mssql

Displays the properties of all mssql profiles.

Options

- **app-service**
  Specifies the name of the application service to which the profile belongs. The default value is **none**. **Note:** If the **strict-updates** option is **enabled** on the application service that owns the object, you cannot modify or delete the profile. Only the application service can modify or delete the profile.
- **defaults-from**
  Specifies the profile that you want to use as the parent profile. Your new profile inherits all settings and values from the parent profile specified. The default value is **mssql**.
- **partition**
  Displays the administrative partition within which the profile resides.
- **read-pool**
  Specifies the pool of MS SQL database servers to which the system sends ready-only requests.
- **read-write-split-by-command**
  When **enabled**, the system decides which pool to send the client requests the by the content in the message. It can only be enabled when read-write-split-by-user is disabled.
- **read-write-split-by-user**
  When **enabled**, the system decides which pool to send the client requests the by user name. It can only be enabled when read-write-split-by-command is disabled.
- **user-can-write-by-default**
  Specifies whether users have write access by default. When set to **true**, all users have write access, except those added to the users list.
- **user-list**
  Specifies the users who have read-only access to the MS SQL if user-can-write-by-default is true, or the users who have write access to the MS SQL database if user-can-write-by-default is false.
- **write_persist_timer**
  Specify how many minimum time in milliseconds the connection will be persisted to write-pool after connection switch to write pool.
- **write-pool**
  Specifies the pool of MS SQL database servers to which the system sends requests that are not read-only.

See Also

create, *delete*, *edit*, glob, *list*, *virtual*, *modify*, regex, *reset-stats*, *show*, *tmsh*

ntlm

Configures a Microsoft® Windows® NT Local Area Network (LAN) manager profile.

Syntax

Configure the **ntlm** component within the **ltm profile** module using the syntax shown in the following sections.

Create/Modify

```
create ntlm [name]
modify ntlm [name]
    app-service [[string] | none]
    defaults-from [name]
    description [string]
    insert-cookie-domain [domain]
    insert-cookie-name [cookie name]
    insert-cookie-passphrase [passphrase]
    key-by-cookie [disabled | enabled]
    key-by-cookie-name [cookie name]
    key-by-domain [disabled| enabled]
    key-by-ip-address [disabled | enabled]
    key-by-target [disabled| enabled]
    key-by-user [disabled | enabled]
    key-by-workstation [disabled| enabled]
edit ntlm [ [ [name] | [glob] | [regex] ] ... ]
   all-properties
   non-default-properties
```

Display

```
list ntlm
list ntlm [ [ [name] | [glob] | [regex] ] ... ]
show running-config ntlm
show running-config ntlm  [ [ [name] | [glob] | [regex] ] ... ]
    all-properties
    non-default-properties
    one-line
    partition
```

Delete

```
delete ntlm [name]
```

Description

You can use the **ntlm** component to create a Microsoft Windows NT LAN manager (NTLM) profile to manage servers on the LAN that are running Windows NT.

Examples

create ntlm my_ntlm_profile defaults-from ntlm

Creates a Microsoft Windows NT LAN manager profile named **my_ntlm_profile** that inherits its settings from the system default NTLM profile named **ntlm**.

list ntlm all-properties

Displays all properties for all NTLM profiles.

Options

- **app-service**
  Specifies the name of the application service to which the profile belongs. The default value is **none**. **Note:** If the **strict-updates** option is **enabled** on the application service that owns the object, you cannot modify or delete the profile. Only the application service can modify or delete the profile.
- **defaults-from**
  Specifies the profile that you want to use as the parent profile. Your new profile inherits all settings and values from the parent profile specified. The default value is **ntlm**.
- **description**
  User defined description.
- **glob**
  Displays the items that match the **glob** expression. See **help glob** for a description of **glob** expression syntax.
- **insert-cookie-domain**
  Specifies an optional domain for the inserted cookie. The default is **none**, which causes no domain to be configured for the inserted cookie.
- **insert-cookie-name**
  Specifies a cookie name that the system inserts in the cookie. The default value is **NTLMconnpool**.
- **insert-cookie-passphrase**
  Specifies a cookie passphrase that the system inserts in the cookie. The default value is **mypassphrase**.
- **key-by-cookie**
  Specifies whether the system uses the existing cookie as the key. The default value is **disabled**.
- **key-by-cookie-name**
  Specifies whether the system uses the value of the **insert-cookie-name** option as the key. The default value is **mycookie**.
- **key-by-domain**
  Specifies whether the system uses the NTLM domain as the key. The default value is **disabled**.

- **key-by-ip-address**
  Specifies whether the system uses the client IP address as the key. The default value is **disabled**.
- **key-by-target**
  Specifies whether the system uses the NTLM target as the key. The default value is **disabled**.
- **key-by-user**
  Specifies whether the system uses the NTLM user as the key. The default value is **enabled**.
- **key-by-workstation**
  Specifies whether the system uses the NTLM workstation as the key. The default value is **disabled**.
- **name**
  Specifies a unique name for the component. This option is required for the commands **create**, **delete**, and **modify**.
- **regex**
  Displays the items that match the regular expression. The regular expression must be preceded by an at sign (@[regular expression]) to indicate that the identifier is a regular expression. See **help regex** for a description of regular expression syntax.

See Also

create, *delete*, *edit*, glob, *list*, *virtual*, *modify*, regex, *reset-stats*, *show*, *tmsh*

ocsp-stapling-params

Configures the OCSP Stapling Parameters object.

Syntax

Configure the **ocsp-stapling-params** component within the **ltm.profile** module using the syntax shown in the following sections. This object is associated with the **certificate** in a **cert-key-chain** object in a **client-ssl** profile to enable OCSP Stapling.

Create/Modify

```
create ocsp-stapling-params [name]
modify ocsp-stapling-params [name]
    cache-error-timeout [integer]
    cache-timeout [indefinite | [integer] ]
    clock-skew [integer]
    dns-resolver [name]
    proxy-server-pool [name]
    responder-url [none | [string] ]
    sign-hash [sha1 | sha256]
    signer-cert [name]
    signer-key [name]
    signer-key-passphrase [none | [string] ]
    status-age [integer]
    strict-resp-cert-check [disabled | enabled]
    timeout [indefinite | [integer] ]
    trusted-ca [name]
    trusted-responders [none | [name] ]
    use-proxy-server [disabled | enabled]
edit ocsp-stapling-params [ [ [name] | [glob] | [regex] ] ... ]
    all-properties
    non-default-properties
```

Display

```
list ocsp-stapling-params
list ocsp-stapling-params [ [ [name] | [glob] | [regex] ] ... ]
```

Delete

```
delete ocsp-stapling-params [name]
```

Description

You can use the **ocsp-stapling-params** component to create, modify, display or delete a custom OCSP Stapling Parameters object.

The OCSP Stapling Parameters object is associated with the certificate in a **cert-key-chain** object of a clientssl profile.

Examples

create ocsp-stapling-params my_ocsp_stapling_params dns-resolver name

Creates an OCSP Stapling Parameters object named **my_ocsp_stapling_params** using the DNS resolver specified by **name**.

create ocsp-stapling-params my_ocsp_stapling_params use-proxy-server enabled proxy-server-pool name

Creates an OCSP Stapling Parameters object named **my_ocsp_stapling_params** using the proxy server pool specified by **name**.

Options

- **cache-error-timeout**
  Specifies the lifetime of an error response in the cache, in seconds. The default value is **3600** seconds.
- **cache-timeout**
  Specifies the lifetime of the OCSP response in the cache, in seconds. The actual time period for which the response is cached is the minimum of the response validity period and the cache-timeout. The default value is **indefinite**, indicating that the response validity period takes precedence.
- **clock-skew**
  Specifies the tolerable absolute difference in the clocks of the responder and the BIG-IP, in seconds. The default value is **300**.
- **dns-resolver**
  Specifies the DNS resolver object used for fetching the OCSP response.
- **proxy-server-pool**
  Specifies the proxy server pool used for fetching the OCSP response.
- **responder-url**
  Specifies the absolute URL that overrides the OCSP responder URL obtained from the certificate's AIA extension(s). This should be a HTTP or HTTPS based URL.
- **sign-hash**
  Specifies the hash algorithm used for signing the OCSP request. The default value is **sha256**.
- **signer-cert**
  Specifies the certificate corresponding to the key used for signing the OCSP request.
- **signer-key**
  Specifies the key used for signing the OCSP request.
- **signer-key-passphrase**
  Specifies the passphrase of the key used for signing the OCSP request.
- **status-age**
  Specifies the allowed age of the OCSP response when nextUpdate time is omitted from the response. The default value is **300**.

- **strict-resp-cert-check**
  If enabled, the responder's certificate is checked for OCSP signing extension. The default value is **disabled**.
- **timeout**
  Specifies the time interval (in seconds) that the BIG-IP waits for before aborting the connection to the OCSP responder. The default value is **8**. The timeout should be less than the handshake timeout of the clientssl profile that the OCSP Stapling Parameters object is associated with.
- **trusted-ca**
  Specifies the certificate-authority that signs the responder's certificate.
- **trusted-responders**
  Specifies the certificate(s) used for validating the OCSP response when the responder's certificate has been omitted from the response.
- **use-proxy-server**
  Specifies whether the proxy server pool or the DNS resolver should be used for the connection to the OCSP responder.

See Also

create, *delete*, *edit*, glob, *list*, *virtual*, *modify*, regex, *tmsh*

one-connect

Configures a OneConnect™ profile.

Syntax

Configure the **one-connect** component within the **ltm profile** module using the syntax shown in the following sections.

Create/Modify

```
create one-connect [name]
modify one-connect [name]
    app-service [[string] | none]
    defaults-from [name]
    description [string]
    idle-timeout-override [disabled | enabled]
    share-pools [disabled | enabled]
    max-age [integer]
    max-reuse [integer]
    max-size [integer]
    source-mask [ip address]
    limit-type [none|idle|strict]
edit one-connect [ [ [name] | [glob] | [regex] ] ... ]
    all-properties
    non-default-properties
mv one-connect [ [[source-name] [destination-name]] | [[name] to-folder [folder-name]]
| [[name...name] to-folder [folder-name]] ]
    to-folder
reset-stats one-connect
reset-stats one-connect[ [ [name] | [glob] | [regex] ] ... ]
```

Display

```
list one-connect
list one-connect [ [ [name] | [glob] | [regex] ] ... ]
show running-config one-connect
show running-config one-connect [ [ [name] | [glob] | [regex] ] ... ]
    all-properties
    non-default-properties
    one-line
    partition
show one-connect
show one-connect [ [ [name] | [glob] | [regex] ] ... ]
    (default | exa | gig | kil | meg | peta | raw | tera | yotta | zetta)
    field-fmt
    global
```

Delete

```
delete one-connect [name]
```

Description

You can use the **one-connect** component to create a OneConnect profile that optimizes connections by improving client performance and increasing server capacity.

Examples

create one-connect my_OC_profile defaults-from oneconnect

Creates a OneConnect profile named **my_OC_profile** that inherits its settings from the system default OneConnect profile named **oneconnect**.

list one-connect all-properties

Displays all properties for all OneConnect profiles.

mv one-connect /Common/my_oneconnect_profile to-folder /Common/my_folder

Moves a custom one-connect profile named **my_oneconnect_profile** to a folder named **my_folder**, where **my_folder** has already been created and exists within **/Common**.

Options

- **app-service**
  Specifies the name of the application service to which the profile belongs. The default value is **none**. **Note:** If the **strict-updates** option is **enabled** on the application service that owns the object, you cannot modify or delete the profile. Only the application service can modify or delete the profile.
- **defaults-from**
  Specifies the profile that you want to use as the parent profile. Your new profile inherits all settings and values from the parent profile specified. The default value is **oneconnect**.
- **description**
  User defined description.
- **glob**
  Displays the items that match the **glob** expression. See **help glob** for a description of **glob** expression syntax.
- **idle-timeout-override**
  Specifies the number of seconds that a connection is idle before the connection flow is eligible for deletion. The default value is **disabled**.
- **share-pools**
  Indicates that connections may be shared not only within a virtual server, but also among similar virtual servers (e.g. those that differ only in destination address). When enabled, all virtual servers that use the same One Connect and other internal network profiles can share connections.

- **max-age**
  Specifies the maximum age, in number of seconds, of a connection in the connection reuse pool. For any connection with an age higher than this value, the system removes that connection from the reuse pool. The default value is **86400**.
- **max-reuse**
  Specifies the maximum number of times that a server connection can be reused. The default value is **1000**.
- **max-size**
  Specifies the maximum number of connections that the system holds in the connection reuse pool. If the pool is already full, then the server connection closes after the response is completed. The default value is **10000**.
- **name**
  Specifies a unique name for the component. This option is required for the commands *create*, *delete*, and *modify*.
- **partition**
  Displays the partition within which the component resides.
- **regex**
  Displays the items that match the regular expression. The regular expression must be preceded by an at sign (@[regular expression]) to indicate that the identifier is a regular expression. See **help regex** for a description of regular expression syntax.
- **source-mask**
  Specifies a source IP mask. The default value is **0.0.0.0**.
  The system applies the value of this option to the source address to determine its eligibility for reuse. A mask of **0.0.0.0** causes the system to share reused connections across all clients. A host mask (all 1's in binary), causes the system to share only those reused connections originating from the same client IP address.
- **limit-type**
  Connection limits with OneConnect are different from straight TCP connection limits. Three options are supported: "none" (the default), "idle", and "strict". When the limit is "none", simultaneous in-flight requests and responses over TCP connections to a pool member are counted toward the limit (this being the historical handling). There may be more TCP connections open to support new requests than there can be simultaneous in-flight requests and responses. This is particularly true when SNAT pools and narrow source address masks are used. When the limit is "idle", idle connections will be dropped as the TCP connection limit is reached. For short intervals, during the overlap of the idle connection being dropped and the new connection being established, the TCP connection limit may be exceeded. When the limit is "strict", the TCP connection limit is honored with no exceptions. This means that idle connections will prevent new TCP connections from being made until they expire, even if they could otherwise be reused. This is not a recommended configuration except in very special cases with short expiration timeouts.

- **to-folder**
  one-connect profiles can be moved to any folder under **/Common**, but configuration dependencies may restrict moving the profile out of **/Common**.

See Also

create, *delete*, *edit*, glob, *list*, *virtual*, *modify*, *mv*, regex, *reset-stats*, *show*, *tmsh*

pcp

Configures a PCP profile.

Syntax

Create/Modify

```
create pcp [name]
modify pcp [name]
    announce-after-failover [ enabled | disabled ]
    announce-multicast [integer]
    app-service [[string] | none]
    defaults-from [ [name] | none]
    description [string]
    map-filter-limit [integer]
    map-limit-per-client [integer]
    map-recycle-delay [integer]
    max-mapping-lifetime [integer]
    min-mapping-lifetime [integer]
    rule [[rule_name] | none]
    third-party-allowed-subnets
      [add | delete | replace-all-with] {
        [ip address/prefix length] ...
    }
    third-party-option [ enabled | disabled ]
edit pcp [ [ [name] | [glob] | [regex] ] ... ]
    all-properties
    non-default-properties
```

Display

```
list pcp
list pcp [ [ [name] | [glob] | [regex] ] ... ]
show running-config pcp
show running-config pcp
  [ [ [name] | [glob] | [regex] ] ... ]
    all-properties
    non-default-properties
    one-line
    partition
```

Delete

```
delete pcp [name]
```

Description

You can use the **pcp** component to specify Port Control Protocol attributes for a profile that can be used in an LSN pool.

Examples

create pcp my_pcp_profile defaults-from pcp

Creates a custom PCP profile named **my_pcp_profile** that inherits its settings from the system default **pcp** profile.

list pcp all-properties

Displays all properties for all PCP profiles.

Options

- **app-service**
  Specifies the name of the application service to which the profile belongs. The default value is **none**.
  Note: If the **strict-updates** option is **enabled** on the application service that owns the object, you cannot modify or delete the profile. Only the application service can modify or delete the profile.
- **defaults-from**
  Specifies the profile that you want to use as the parent profile. Your new profile inherits all settings and values from the parent profile specified. The default value is **pcp**, a profile that is shipped in the software.
- **description**
  User defined description.
- **announce-after-failover**
  Specifies that the BIG-IP software should send an unsolicited ANNOUNCE response to all PCP clients when there is a failover. The unsolicited ANNOUNCE response goes over a link-local multi-cast address, and it contains a new EPOCH time. This signals to the PCP clients that they should renew all of their active mappings.
- **announce-multicast**
  Whenever the BIG-IP system reboots, or if there is any possibility that the system lost its PCP-mapping state, it sends an unsolicited ANNOUNCE response to all of its PCP clients. It sends the response over a link-local multi-cast address, and it contains a new EPOCH time. The PCP clients react by renewing all of their active IP mappings. To compensate for possible packet loss (since the multi-cast address is link-local), you can use this property to set the number of multi-cast re-sends. Default is 10 re-sends.
- **map-filter-limit**
  A PCP client can request a "filter" for a mapping entry, where the filter limits the number of external endpoints that can use the IP map. The filter request contains the particular IP address and port for the endpoint (or subnet of endpoints), as well as a prefix length. Enter the maximum number of filters (allowed subnets) that clients are allowed to set for each PCP mapping. Default is 1.
- **map-limit-per-client**
  Specifies the maximum number of PCP mappings per client. Default is 65535 (unlimited).

Use **run util lsndb** to see the currently-active set of PCP mappings on the system. See *lsndb* for details on the LSN DB utility.

- **map-recycle-delay**
  After a IP mapping times out (that is, its lifetime expires), there is a further delay before the public-side address and port can be used by another PCP client. Use this property to set the recycle delay. Default is 60 (seconds).
  Use **run util lsndb** to see the currently-active set of PCP mappings on the system. See *lsndb* for details on the LSN DB utility.
- **max-mapping-lifetime**
  When a PCP client requests an IP mapping from a BIG IP system, it also requests a "lifetime" for the mapping. The mapping expires at the end of that lifetime. This property is the maximum number of seconds allowed for a mapping lifetime. Default is 86400 (seconds), or 1 day.
  Use **run util lsndb** to see the currently-active set of PCP mappings on the system. See *lsndb* for details on the LSN DB utility.
- **min-mapping-lifetime**
  Specifies the minimum number of seconds allowed for a mapping lifetime. Default is 600 (seconds), or 10 minutes.
  Use **run util lsndb** to see the currently-active set of PCP mappings on the system. See *lsndb* for details on the LSN DB utility.
- **regex**
  Displays the items that match the regular expression. The regular expression must be preceded by an at sign (@[regular expression]) to indicate that the identifier is a regular expression. See **help regex** (regex) for a description of regular expression syntax.
- **rule**
  Specifies the iRule that is associated with this pcp profile. An iRule can read packets and possibly filter them based on whatever programming logic you design. For example, an iRule could reject all PCP mapping requests using a specific port, or pass an ANNOUNCE request through a specific port. An iRule gives you the flexibility to filter, process, or log the PCP packets that fit this profile.
  Select an iRule from the menu of existing iRules. To create a new one, use the **create ltm rule** command (see *rule*).
- **third-party-allowed-subnets**
  Specifies the PCP clients that can make MAP requests on behalf of other clients. Enter a collection of IP prefixes (IPv4 or IPv6) with their prefix lengths. If a PCP client outside of any of these subnets attempts a PCP mapping, the BIG-IP software rejects the mapping.
  You can shorten any IPv6 addresses as defined in RFC 2373 (see http://www.ietf.org/rfc/rfc2373.txt).
  This list is only used if the **third-party-option** is also enabled.
  If the list is empty and the **third-party-option** is enabled, any PCP client can create mappings for third parties.
- **third-party-option**
  Allows PCP clients to make MAP requests on behalf of other clients, using the THIRD_PARTY flag in the PCP request. You can set this property to **enabled** or **disabled**. If you enable this property, we

recommend using the **third-party-subnets** option to limit the the clients that can use the THIRD_PARTY flag; it is a potential security risk. The default is disabled.

See Also

create, *delete*, *edit*, *list*, *lsn-pool*, *modify*, *tmsh*

pptp

Configures a Point-to-Point Tunneling Protocol (PPTP) profile.

Syntax

Configure the **pptp** component within the **ltm profile** module using the syntax shown in the following sections.

Create/Modify

```
create pptp [name]
modify pptp [name]
    app-service [[string] | none]
    defaults-from [ [name] | none]
    description [[string] | none]
    publisher-name [[string] | none]
    include-destination-ip [disabled | enabled]
edit pptp [ [ [name] | [glob] | [regex] ] ... ]
    all-properties
    non-default-properties
reset-stats pptp
reset-stats pptp [ [ [name] | [glob] | [regex] ] ... ]
```

Display

```
list pptp
list pptp [ [ [name] | [glob] | [regex] ] ... ]
show running-config pptp
show running-config pptp [ [ [name] | [glob] | [regex] ] ... ]
    all-properties
    non-default-properties
    one-line
    partition
show pptp
show pptp [ [ [name] | [glob] | [regex] ] ... ]
    (default | exa | gig | kil | meg | peta | raw | tera | yotta | zetta)
    field-fmt
```

Delete

```
delete pptp [name]
```

Description

You can use the **pptp** component to manage a PPTP profile.

Examples

create pptp my_pptp_profile defaults-from pptp

Creates a PPTP profile named **my_pptp_profile** using the system defaults.

create pptp my_pptp_profile { log-server-ip disabled }

Creates a PPTP profile named **my_pptp_profile** with server address logging disables.

modify pptp my_pptp_profile description "This is a PPTP Profile"

Modifies the description attribute of a PPTP profile named **my_pptp_profile**.

Options

- **app-service**
  Specifies the name of the application service to which the object belongs. The default value is **none**.
- **defaults-from**
  Specifies the profile that you want to use as the parent profile. Your new profile inherits all of the settings and values from the specified parent profile. The default value is **pptp**.
- **description**
  User defined description.
- **glob**
  Displays the items that match the **glob** expression. See **help glob** for a description of **glob** expression syntax.
- **publisher-name**
  Specifies the name of the log publisher for PPTP events.
- **include-destination-ip**
  Specifies whether the log messages for call establishment/disconnect include the server's ip address. The default value is **disabled**. When disabled the ip address will be displayed as 0.0.0.0.
- **name**
  Specifies a unique name for the component. This option is required for the commands **create**, **delete**, and **modify**.
- **partition**
  Displays the administrative partition within which the component resides.
- **regex**
  Displays the items that match the regular expression. The regular expression must be preceded by an at sign (@[regular expression]) to indicate that the identifier is a regular expression. See **help regex** for a description of regular expression syntax.

See Also

create, *delete*, *edit*, glob, *list*, *virtual*, *modify*, regex, *reset-stats*, *show*, *tmsh*

qoe

Configures a Quality of Experience (QoE) Monitoring profile.

Syntax

Configure the **qoe** component within the **ltm profile** module using the syntax shown in the following sections.

Create/Modify

```
create qoe [name]
modify qoe [name]
    video [true/false]
reset-stats qoe
reset-stats qoe [ [ [name] | [glob] | [regex] ] ... ]
```

Display

```
list qoe
list qoe [ [ [name] | [glob] | [regex] ] ... ]
show running-config qoe
show running-config qoe [ [ [name] | [glob] | [regex] ] ... ]
    all-properties
    non-default-properties
    one-line
    partition
show qoe
show qoe [ [ [name] | [glob] | [regex] ] ... ]
    (default | exa | gig | kil | meg | peta | raw | tera | yotta | zetta)
    field-fmt
```

Delete

```
delete qoe [name]
```

Description

You can use the **qoe** component to monitor Video Quality of Experience.

Examples

create qoe my_qoe defaults-from qoe

Creates an quality of experience profile named **my_qoe**.

create qoe my_qoe { video true }

- **video**
  Specifies to monitor the QoE MOS score of video streams with the format of MP4 or FLV.

See Also

create, *delete*, *edit*, glob, *list*, *virtual*, *modify*, regex, *reset-stats*, *show*, *tmsh*, *qoe*

radius

Configures a RADIUS profile for network traffic load balancing.

Syntax

Configure the **radius** component within the **ltm profile** module using the syntax shown in the following sections.

Create/Modify

```
create radius [name]
modify radius [name]
    app-service [[string] | none]
    clients [add | delete | modify | replace-all-with] {
      [ip address] ...
     }
    clients none
    defaults-from [name]
    description [string]
    persist-avp [ [string] | [integer] | none]
    subscriber-aware [ disabled | enabled ]
    subscriber-id-type [3gpp-imsi | calling-station-id | user-name]
mv radius [ [[source-name] [destination-name]] | [[name] to-folder [folder-name]] |
[[name...name] to-folder [folder-name]] ]
    to-folder
edit radius [ [ [name] | [glob] | [regex] ] ... ]
   all-properties
   non-default-properties
reset-stats radius
reset-stats radius [ [ [name] | [glob] | [regex] ] ... ]
```

Display

```
list radius
list radius [ [ [name] | [glob] | [regex] ] ... ]
show running-config radius
show running-config radius [ [ [name] | [glob] | [regex] ] ... ]
    all-properties
    non-default-properties
    one-line
    partition
show radius
show radius [ [ [name] | [glob] | [regex] ] ... ]
    (default | exa | gig | kil | meg | peta | raw | tera | yotta | zetta)
    field-fmt
    global
```

Delete

```
delete radius [name]
```

Description

You can use the **radius** component to manage RADIUS network traffic.

Examples

create radius my_radius_server

Creates a RADIUS profile named **my_radius_server** that inherits its settings from the system default RADIUS profile.

delete radius my_radius_server

Deletes the RADIUS profile named **my_radius_server**.

mv radius /Common/my_radius_profile to-folder /Common/my_folder

Moves a custom radius profile named **my_radius_profile** to a folder named **my_folder**, where **my_folder** has already been created and exists within **/Common**.

Options

- **app-service**
  Specifies the name of the application service to which the profile belongs. The default value is **none**. **Note:** If the **strict-updates** option is **enabled** on the application service that owns the object, you cannot modify or delete the profile. Only the application service can modify or delete the profile.
- **clients**
  Specifies host and network addresses from which clients can connect. The default value is **none**, which indicates that any client can connect.
- **defaults-from**
  Specifies the profile that you want to use as the parent profile. Your new profile inherits all settings and values from the parent profile. The default value is **radiusLB**.
- **description**
  User defined description.
- **glob**
  Displays the items that match the **glob** expression. See **help glob** for a description of **glob** expression syntax.
- **name**
  Specifies a unique name for the component. This option is required for the commands **create**, **delete**, and **modify**.
- **partition**
  Displays the administrative partition within which the component resides.

- **persist-avp**
  Specifies the name of the RADIUS attribute on which traffic persists. Acceptable values are ASCII strings from section 5 of RFC 2865 or numeric codes (1-255). The default value is **none**, which indicates that persistence is disabled.
- **regex**
  Displays the items that match the regular expression. The regular expression must be preceded by an at sign (@[regular expression]) to indicate that the identifier is a regular expression. See **help regex** for a description of regular expression syntax.
- **subscriber-aware**
  Specifies whether to extract subscriber information from RADIUS packets. The options are **disabled** and **enabled**. The default value is **disabled**, which indicates that it will not extract subscriber information from RADIUS packets.
- **subscriber-id-type**
  Specifies the RADIUS attribute to be used as the subscriber Id when extracting subscriber information from the RADIUS message. This field is ignored if **subscriber-aware** is **disabled**. The options are **3gpp-imsi**, indicates that 3GPP-IMSI RADIUS sub-attribute (26/10415.1) is used as subscriber Id; **calling-station-id**, indicates that Calling-Station-Id RADIUS attribute(#31) is used as subscriber Id; and **user-name**, indicates that User-Name RADIUS attribute(#1) is used as subscriber Id. The default value is **3gpp-imsi**.
- **to-folder**
  radius profiles can be moved to any folder under **/Common**, but configuration depenedencies may restrict moving the profile out of **/Common**.

See Also

create, *delete*, *edit*, glob, *list*, *virtual*, *modify*, *mv*, regex, *reset-stats*, *show*, *tmsh*

ramcache

Manages the BIG-IP® system RAM cache.

Syntax

Configure the **ramcache** component within the **ltm profile** module using the syntax shown in the following sections.

Display

```
show ramcache
show ramcache [ [ [name] | [glob] | [regex] ] ... ]
    exact
    host [string]
    max-response [integer]
    uri [string]
```

Delete

```
delete ramcache [name]
```

Description

You can use the **ramcache** component to delete the entries in or show information about the BIG-IP® system RAM cache.

Examples

show ramcache

Displays information about the entries in the BIG-IP system RAM cache.

delete ramcache

Deletes the entries in the BIG-IP system RAM cache.

Options

- **exact**
  Displays the exact number of entries in the RAM cache.
- **host**
  Displays the host from which the entry was cached.
- **max-response**
  Displays the maximum number of entries that can be in the RAM cache. The default value is **0** (zero), which means that the system does not limit the maximum entries.

- **regex**
  Displays the items that match the regular expression. The regular expression must be preceded by an at sign (@[regular expression]) to indicate that the identifier is a regular expression. See **help regex** for a description of regular expression syntax.
- **uri**
  Displays the URI from which the entry was cached.

See Also

delete, *show*, *tmsh*

request-adapt

Configures a HTTP request adaptation profile.

Syntax

Configure the **request-adapt** component within the **ltm profile** module using the syntax shown in the following sections.

Create/Modify

```
create request-adapt [name]
modify request-adapt [name]
    defaults-from [ [name] | none]
    enabled [ yes | no ]
    internal-virtual [ [name] | none]
    preview-size [integer]
    service-down-action [ ignore | reset | drop ]
    timeout [integer]
    allow-http-10 [ yes | no ]
edit request-adapt [ [ [name] | [glob] | [regex] ] ... ]
    all-properties
    non-default-properties
mv request-adapt [ [[source-name] [destination-name]] | [[name] to-folder
[folder-name]] | [[name...name] to-folder [folder-name]] ]
    to-folder
reset-stats request-adapt
reset-stats request-adapt [ [ [name] | [glob] | [regex] ] ... ]
```

Display

```
list request-adapt
list request-adapt [ [ [name] | [glob] | [regex] ] ... ]
show running-config request-adapt
show running-config request-adapt [ [ [name] | [glob] | [regex] ] ... ]
    all-properties
    non-default-properties
    one-line
    partition
show request-adapt
show request-adapt [ [ [name] | [glob] | [regex] ] ... ]
    (default | exa | gig | kil | meg | peta | raw | tera | yotta | zetta)
    field-fmt
```

Delete

```
delete request-adapt [name]
```

Description

You can use the **request-adapt** component to manage a HTTP request adaptation profile.

Examples

create request-adapt my_req_adapt defaults-from request-adapt

Creates a HTTP request adaptation profile named **my_req_adapt** using the system defaults.

create request-adapt my_req_adapt { enabled yes }

Creates a HTTP request adaptation profile named **my_req_adapt** that is enabled for adapting HTTP requests.

mv request-adapt /Common/my_requestadapt_profile to-folder /Common/my_folder

Moves a custom request-adapt profile named **my_requestadapt_profile** to a folder named **my_folder**, where **my_folder** has already been created and exists within **/Common**.

- **defaults-from**
  Specifies the profile that you want to use as the parent profile. Your new profile inherits all of the settings and values from the specified parent profile. The default value is **requestadapt**.
- **enabled**
  Enables adaptation of HTTP requests. If set to **yes**, HTTP requests will be forwarded to the specified internal virtual server for adaptation. The default value is **yes**.
- **internal-virtual**
  Specifies the name of the internal virtual server to use for adapting the HTTP request.
- **preview-size**
  Specifies the maximum size of the preview buffer. The preview buffer is used to hold a copy of the HTTP request header and data sent to the internal virtual server in case the adaptation server reports that it does not need to adapt the HTTP request. Setting the preview-size to **0**, disables buffering the request and should only be done if the adaptation server will always return with a modified HTTP request or the original HTTP request. The default value is **1024**.
- **service-down-action**
  Specifies the action to take if the internal virtual server does not exist or returns an error. The default value is **ignore**.
  The options are:
  - **ignore**
    Ignore the error and send the unmodified HTTP request to a HTTP server selected from this virtual server's pool.
  - **drop**
    Drop the connection.
  - **reset**
    Reset the connection.
- **timeout**
  Specifies a timeout in milliseconds. If the internal virtual server does not return a result within the specified time, a timeout error will occur. A **0** value disables the timeout. The default value is **0**.

- **to-folder**
  request-adapt profiles can be moved to any folder under **/Common**, but configuration depenedencies may restrict moving the profile out of **/Common**.
- **allow-http-10**
  Specifies whether to forward HTTP version 1.0 requests for adaptation. By default only HTTP version 1.1 requests are forwarded. Version 1.0 is not supported. While it should work in most cases, it might be necessary to restrict adaptation on a site-specific basis. The default value is **no**.

See Also

create, *delete*, *edit*, glob, *list*, *virtual*, *modify*, *mv*, regex, *reset-stats*, *show*, *tmsh*, *response-adapt*

request-log

Configures a Request-Logging profile.

Syntax

Configure the **request-log** component within the **ltm profile** module using the syntax shown in the following sections.

Create/Modify

```
create request-log [name]
modify request-log [name]
    app-service [[string] | none]
    defaults-from [[name] | none]
    description [string]
    log-request-logging-errors [disabled | enabled]
    log-response-by-default [disabled | enabled]
    log-response-logging-error [disabled | enabled]
    proxy-close-on-error [disabled | enabled]
    proxy-respond-on-logging-error [disabled | enabled]
    proxy-response [string]
    request-log-error-pool [ [pool_name] | none]
    request-log-error-protocol [ TCP | UDP | none]
    request-log-error-template [string]
    request-log-pool [ [pool_name] | none]
    request-log-protocol [ TCP | UDP | none]
    request-log-template [string]
    request-logging [disabled | enabled]
    response-log-error-pool [ [pool_name] | none]
    response-log-error-protocol [ TCP | UDP | none]
    response-log-error-template [string]
    response-log-pool [ [pool_name] | none]
    response-log-protocol [ TCP | UDP | none]
    response-log-template [string]
    response-logging [disabled | enabled]
edit request-log [ [ [name] | [glob] | [regex] ] ... ]
    all-properties
    non-default-properties
mv request-log [ [[source-name] [destination-name]] | [[name] to-folder [folder-name]]
| [[name...name] to-folder [folder-name]] ]
    to-folder
```

Display

```
list request-log
list request-log [ [ [name] | [glob] | [regex] ] ... ]
show running-config request-log
show running-config request-log
  [ [ [name] | [glob] | [regex] ] ... ]
    all-properties
    non-default-properties
    one-line
    partition
```

```
show request-log
show request-log [ [ [name] | [glob] | [regex] ] ... ]
    (default | exa | gig | kil | meg | peta | raw | tera | yotta | zetta)
    field-fmt
    global
```

Delete

```
delete request-log [name]
```

Description

You can use the **request-log** component to manage request-log network traffic.

Examples

create request-log my_reqlog_profile defaults-from request-log

Creates a custom **request-log** profile named **my_reqlog_profile** that inherits its settings from the system default **request-log** profile.

list request-log all-properties

Displays all properties for all **request-log** profiles.

mv request-log /Common/my_requestlog_profile to-folder /Common/my_folder

Moves a custom request-log profile named **my_requestlog_profile** to a folder named **my_folder**, where **my_folder** has already been created and exists within **/Common**.

Options

- **app-service**
  Specifies the name of the application service to which the profile belongs. The default value is **none**. **Note:** If the **strict-updates** option is **enabled** on the application service that owns the object, you cannot modify or delete the profile. Only the application service can modify or delete the profile.
- **defaults-from**
  Specifies the default values from this profile.
- **description**
  User defined description.
- **log-request-logging-errors**
  Enables secondary logging should the primary lack sufficient available bandwidth. This mechanism is best used to send an alert to a completely separate destination.

- **log-response-by-default**
  Indicates if response logging may be overridden via iRule. This field determines the default response action.
- **log-response-logging-errors**
  Enables secondary logging should the primary lack sufficient available bandwidth. This mechanism is best used to send an alert to a completely separate destination.
- **partition**
  Displays the administrative partition within which the profile resides.
- **proxy-close-on-error**
  Specifies, if enabled, that the logging profile will close the connection after sending its proxy-response.
- **proxy-respond-on-logging-error**
  Specifies that the logging profile respond directly (for example, with an HTTP 502) if the logging fails.
- **proxy-response**
  Specifies the response to send on logging errors.
- **regex**
  Displays the items that match the regular expression. The regular expression must be preceded by an at sign (@[regular expression]) to indicate that the identifier is a regular expression. See **help regex** for a description of regular expression syntax.
- **request-log-error-pool**
  Specifies the name of the pool from which to select log servers.
- **request-log-error-protocol**
  Specifies the HighSpeedLogging protocol to use when logging.
- **request-log-error-template**
  Specifies the template to use when generating log messages. Shell style escapes (for example, $foo and/or ${foo}) are used to import transaction-specific values.
- **request-log-pool**
  Specifies the name of the pool from which to select log servers.
- **request-log-protocol**
  Specifies the HighSpeedLogging protocol to use when logging.
- **request-log-template**
  Specifies the template to use when generating log messages. Shell style escapes (for example, $foo and/or ${foo}) are used to import transaction-specific values.
- **request-logging**
  Enables or disables logging before the response is returned to the client.
- **response-log-error-pool**
  Specifies the name of the pool from which to select log servers.
- **response-log-error-protocol**
  Specifies the HighSpeedLogging protocol to use when logging.

- **response-log-error-template**
  Specifies the template to use when generating log messages. Shell style escapes (for example, $foo and/or ${foo}) are used to import transaction-specific values.
- **response-log-pool**
  Specifies the name of the pool from which to select log servers.
- **response-log-protocol**
  Specifies the HighSpeedLogging protocol to use when logging.
- **response-log-template**
  Specifies the template to use when generating log messages. Shell style escapes (for example, $foo and/or ${foo}) are used to import transaction-specific values.
- **response-logging**
  Enables or disables logging before the response is returned to the client.
- **to-folder**
  request-log profiles can be moved to any folder under **/Common**, but configuration depenedencies may restrict moving the profile out of **/Common**.

See Also

create, *delete*, *edit*, glob, *ltm profile*, *virtual*, *modify*, *mv*, *show*, regex, *tmsh*

response-adapt

Configures a HTTP response adaptation profile.

Syntax

Configure the **response-adapt** component within the **ltm profile** module using the syntax shown in the following sections.

Create/Modify

```
create response-adapt [name]
modify response-adapt [name]
    defaults-from [ [name] | none]
    enabled [ yes | no ]
    internal-virtual [ [name] | none]
    preview-size [integer]
    service-down-action [ ignore | reset | drop ]
    timeout [integer]
    allow-http-10 [ yes | no ]
edit response-adapt [ [ [name] | [glob] | [regex] ] ... ]
    all-properties
    non-default-properties
mv response-adapt [ [[source-name] [destination-name]] | [[name] to-folder
[folder-name]] | [[name...name] to-folder [folder-name]] ]
    to-folder
reset-stats response-adapt
reset-stats response-adapt [ [ [name] | [glob] | [regex] ] ... ]
```

Display

```
list response-adapt
list response-adapt [ [ [name] | [glob] | [regex] ] ... ]
show running-config response-adapt
show running-config response-adapt [ [ [name] | [glob] | [regex] ] ... ]
    all-properties
    non-default-properties
    one-line
    partition
show response-adapt
show response-adapt [ [ [name] | [glob] | [regex] ] ... ]
    (default | exa | gig | kil | meg | peta | raw | tera | yotta | zetta)
    field-fmt
```

Delete

```
delete response-adapt [name]
```

Description

You can use the **response-adapt** component to manage a HTTP response adaptation profile.

Examples

create response-adapt my_req_adapt defaults-from response-adapt

Creates a HTTP response adaptation profile named **my_req_adapt** using the system defaults.

create response-adapt my_req_adapt { enabled yes }

Creates a HTTP response adaptation profile named **my_req_adapt** that is enabled for adapting HTTP responses.

mv response-adapt /Common/my_responseadapt_profile to-folder /Common/my_folder

Moves a custom responseadapt profile named **my_responseadapt_profile** to a folder named **my_folder**, where **my_folder** has already been created and exists within **/Common**.

- **defaults-from**
  Specifies the profile that you want to use as the parent profile. Your new profile inherits all of the settings and values from the specified parent profile. The default value is **responseadapt**.
- **enabled**
  Enables adaptation of HTTP responses. If set to **yes**, HTTP responses will be forwarded to the specified internal virtual server for adaptation. The default value is **yes**.
- **internal-virtual**
  Specifies the name of the internal virtual server to use for adapting the HTTP response.
- **preview-size**
  Specifies the maximum size of the preview buffer. The preview buffer is used to hold a copy of the HTTP response header and data sent to the internal virtual server in case the adaptation server reports that it does not need to adapt the HTTP response. Setting the preview-size to **0**, disables buffering the response and should only be done if the adaptation server will always return with a modified HTTP response or the original HTTP response. The default value is **1024**.
- **service-down-action**
  Specifies the action to take if the internal virtual server does not exist or returns an error. The default value is **ignore**.
  The options are:
  - **ignore**
    Ignore the error and send the unmodified HTTP response to a HTTP server selected from this virtual server's pool.
  - **drop**
    Drop the connection.
  - **reset**
    Reset the connection.
- **timeout**
  Specifies a timeout in milliseconds. If the internal virtual server does not return a result within the specified time, a timeout error will occur. A **0** value disables the timeout. The default value is **0**.

- **to-folder**
  response-adapt profiles can be moved to any folder under **/Common**, but configuration depenedencies may restrict moving the profile out of **/Common**.
- **allow-http-10**
  Specifies whether to forward HTTP version 1.0 responses for adaptation. By default only HTTP version 1.1 responses are forwarded. Version 1.0 is not supported. While it should work in most cases, it might be necessary to restrict adaptation on a site-specific basis. The default value is **no**.

See Also

create, *delete*, *edit*, glob, *list*, *virtual*, *modify*, *mv*, regex, *reset-stats*, *show*, *tmsh*, *request-adapt*

rewrite

configure a rewrite profile

Syntax

Configure the **rewrite** component within the **profile** module using the syntax shown in the following sections.

Display

```
list rewrite
list rewrite [[name] | [glob]]
show running-config rewrite
show running-config rewrite [[name] | [glob]]
    all-properties
    non-default-properties
    one-line
    | grep
```

Create/Modify

```
create rewrite [name]
modify rewrite [name]
    app-service [[string] | none]
    bypass-list [add | delete | replace-all-with | none] { [uri list] }
    client-caching-type [cache-all | cache-css-js | cache-img-css-js | no-cache]
    defaults-from [[name] | none]
    java-ca-file [[certificate file] | none]
    java-crl [[certificate revocation list file] | none]
    java-sign-key [[certificate key file] | none]
    java-sign-key-passphrase [[string] | none]
    java-signer [[certificate file] | none]
    location-specific [false | true]
    rewrite-list [add | delete | replace-all-with | none] { [uri list] }
    rewrite-mode [portal | uri-translation]
    set-cookie-rules [add | delete | modify | replace-all-with | none] {
      [name] {
        client {
          domain [string]
          path [string]
        }
        server {
          domain [string]
          path [string]
        }
      }
    }
    split-tunneling [false | true]
    uri-rules [add | delete | modify | replace-all-with | none] {
      [name] {
        [type [both | request | response]]
        client {
          scheme [string]
          host [string]
          port [string]
          path [string]
```

```
          }
          server {
            scheme [string]
            host [string]
            port [string]
            path [string]
          }
        }
      }
edit rewrite [ [ [name] | [glob] ] ... ]
    all-properties
    non-default-properties
```

Delete

```
delete rewrite [name]
```

Description

Use the **rewrite** component to configure a Rewrite Profile in URI Translation or Portal (Access) mode.

Examples

- **URI Translation Mode**

- Create a profile
  create my_uri_rewrite rewrite-mode uri-translation
- Add a rule to rewrite URIs
  modify my_uri_rewrite uri-rules add { my_rule { client { path /client/ } server { path /server/ } } }
  modify my_uri_rewrite uri-rules add { my_rule { client { scheme http host www.client.com path / } server { scheme http host www.server.com path / } } }
- Add a rule to rewrite Set-Cookie headers
  modify my_uri_rewrite set-cookie-rules add { my_rule { client { domain client.com path / } server { domain server.com path / } } }
- **Portal (Access) Mode**

- Create a profile
  create my_portal_rewrite rewrite-mode portal
- Configure the client to cache all files
  modify my_portal_rewrite client-caching-type cache-all
- Set the rewrite list and bypass list
  modify my_portal_rewrite rewrite-list add { *://www.myportal.com/* http://abc*.com/* } bypass-list add { *://external_web.com/* }
- Configure split-tunneling
  modify my_portal_rewrite split-tunneling true

Options

- **app-service**
  Specifies the name of the application service to which the object belongs. The default value is **none**. **Note:** If the **strict-updates** option is **enabled** on the application service that owns the object, you cannot modify or delete the object. Only the application service can modify or delete the object.
- **bypass-list**
  Specifies a list of URIs that are bypassesed inside a web page when the page is accessed using Portal Access. The default is **none**.
- **client-caching-type**
  Specifies one of four options for client caching. When the Client Cache setting for a web application resource is set to **default**, the system uses the setting configured in the Rewrite profile. If the Client Cache option is configured for any other setting, the web application resource item caching configuration overwrites the setting in the Rewrite profile. The default is **cache-css-js**. The options are:
  - **cache-all**
    Do not modify cache headers on backend servers.
  - **cache-css-js**
    Cache only the CSS file and Java Script.
  - **cache-img-css-js**
    Cache only images, the CSS file and Java Script.
  - **no-cache**
    Eliminate caching.
- **defaults-from**
  Specifies the profile from which the Rewrite profile inherits properties. Explicitly specified properties override inherited properties.
- **java-ca-file**
  Specifies a CA against which to verify signed Java applets signatures. The default value is **ca-bundle.crt**.
- **java-crl**
  Specifies a CRL against which to verify signed Java applets signature certificates. The default value is **none**.
- **java-sign-key**
  Specifies a private key for re-signing of signed Java applets after patching. The default value is **default.key**.
- **java-sign-key-passphrase**
  Specifies a passphrase for the private key to be encrypted with. The default value is **none**. **Note:** your passphrase will be encrypted and displayed under the label **java-sign-key-passphrase-encrypted**.
- **java-signer**
  Specifies a certificate to use for re-signing of signed Java applets after patching. The default value is **default.crt**.

- **location-specific**
  Specifies whether or not this object contains one or more attributes with values that are specific to the location where the BIG-IP device resides. The location-specific attribute is either true or false. When using policy sync, mark an object as location-specific to prevent errors that can occur when policies reference objects, such as authentication servers, that are specific to a certain location. The default value is **none**.
- **rewrite-list**
  Specifies a list of URIs that are rewritten inside a web page when the page is accessed using Portal Access. The default value is **none**.
- **rewrite-mode**
  Specifies the mode of rewriting. **uri-translation** is a rules-based rewrite mode. **portal** is for use with Portal Access.
- **set-cookie-rules**
  Used with **uri-translation** mode. Specifies the rules for rewriting HTTP Set-Cookie headers. Each rule has a name and a client and server domain and path. The name may be any alphanumeric string and must be unique. The path must be an absolute directory path and not a relative path or a file path. If the domain and path of the Set-Cookie header in the HTTP response match the domain and path of the server side of a rule, they will be rewritten to the domain and path of client side of that rule. Set-Cookie rules take precedence over URI rules when rewriting Set-Cookie headers.
- **split-tunneling**
  Specifies whether the profile provides for split tunneling. The default is **false**.
- **uri-rules**
  Used with **uri-translation** mode. Specifies the rules for rewriting request and response headers and response bodies. These rules affect the following.
  - **request headers**
    URI, Host, Referer
  - **response headers**
    Content-Location, Link, Location, Refresh, Set-Cookie
  - **response body**
    HTML, CSS

  Each rule has a name, a type, and a client and server URI. The name may be any alphanumeric string and must be unique. The type may be "request", "response", or "both": "request" rules affect request headers only, "response" rules affect response headers and bodies only, and "both" rules affect both. URIs must include a path; scheme, host, and port are optional. If a URI must contain a scheme or host, it must include both. If it must include a port, it must also include a scheme and host. Paths may be absolute directory paths only. They may not be relative paths or file paths. If a URI in a request header matches the client side URI of a rule, it will be rewritten to the server side URI of that rule. If a URI in a response header or body matches the server side URI of a rule, it will be rewritten to the client side URI of that rule. When rewriting Set-Cookie headers, the host and path of the server side URI are used to match the domain and path of the header. The client

side host and path replace that header's domain and path if a match is found. Set-Cookie rules take precedence over URI rules when rewriting Set-Cookie headers.

rtsp

Configures an RTSP (realtime streaming protocol) profile.

Syntax

Configure the **rtsp** component within the **ltm profile** module using the syntax shown in the following sections.

Create/Modify

```
create rtsp [name]
modify rtsp [name]
    app-service [[string] | none]
    check-source [disabled | enabled]
    defaults-from [name]
    description [string]
    idle-timeout [integer]
    max-header-size [integer]
    max-queued-data [integer]
    multicast-redirect [disabled | enabled]
    proxy [external | internal | none]
    proxy-header [ [name] | none]
    real-http-persistence [disabled | enabled]
    rtcp-port [number]
    rtp-port [number]
    session-reconnect [disabled | enabled]
    unicast-redirect [disabled | enabled]
    log-publisher [log publisher name | none]
    log-profile [log profile name | none]
edit rtsp [ [ [name] | [glob] | [regex] ] ... ]
    all-properties
    non-default-properties
mv rtsp [ [[source-name] [destination-name]] | [[name] to-folder [folder-name]] |
[[name...name] to-folder [folder-name]] ]
    to-folder
reset-stats rtsp
reset-stats rtsp [ [ [name] | [glob] | [regex] ] ... ]
```

Display

```
list rtsp
list rtsp [ [ [name] | [glob] | [regex] ] ... ]
show running-config rtsp
show running-config rtsp
  [ [ [name] | [glob] | [regex] ] ... ]
    all-properties
    non-default-properties
    one-line
    partition
show rtsp
show rtsp [ [ [name] | [glob] | [regex] ] ... ]
    (default | exa | gig | kil | meg | peta | raw | tera | yotta | zetta)
    field-fmt
    global
```

Delete

```
delete rtsp [name]
```

Description

You can use the **rtsp** component to manage a profile that you use to control RTSP traffic.

Examples

create rtsp my_rtsp_profile defaults-from rtsp

Creates a custom RTSP profile named **my_rtsp_profile** that inherits its settings from the system default RTSP profile.

list rtsp all-properties

Displays all properties for all RTSP profiles.

mv rtsp /Common/my_rtsp_profile to-folder /Common/my_folder

Moves a custom rtsp profile named **my_rtsp_profile** to a folder named **my_folder**, where **my_folder** has already been created and exists within **/Common**.

Options

- **app-service**
  Specifies the name of the application service to which the profile belongs. The default value is **none**. **Note:** If the **strict-updates** option is **enabled** on the application service that owns the object, you cannot modify or delete the profile. Only the application service can modify or delete the profile.
- **check-source**
  When **enabled** the system uses the source attribute in the transport header to establish the target address of the RTP stream, and before the response is forwarded to the client, updates the value of the source attribute to be the virtual address of the BIG-IP system. When **disabled** the system does not change the source attribute. The default value is **enabled**.
- **defaults-from**
  Specifies the profile that you want to use as the parent profile. Your new profile inherits all of the settings and values from the specified parent profile. The default value is **rtsp**.
- **description**
  User defined description.
- **glob**
  Displays the items that match the **glob** expression. See **help glob** for a description of **glob** expression syntax.

- **idle-timeout**
  Specifies the number of seconds that a connection is idle before the connection is eligible for deletion. The default value is **300** seconds.
- **max-header-size**
  Specifies the maximum size of an RTSP request or response header that the RTSP filter accepts before dropping the connection. The default value is **4096** bytes.
- **max-queued-data**
  Specifies the maximum amount of data that the RTSP filter buffers before dropping the connection. The default value is **32768** bytes.
- **multicast-redirect**
  Specifies whether to enable or disable multicast redirect. When enabled, the client can select the destination to which to stream data. The default value is **disabled**.
- **name**
  Specifies a unique name for the component. This option is required for the commands **create**, **delete**, and **modify**.
- **partition**
  Displays the administrative partition within which the component resides.
- **proxy**
  Specifies whether the RTSP filter is associated with an RTSP proxy configuration. The default value is **none**.
- **proxy-header**
  When the **proxy** option is set, specifies the name of the header in the RTSP proxy configuration that is passed from the client-side virtual server to the server-side virtual server. Note that the name of the header must begin with **X-**. The default value is **none**.
  To use the proxy-header option, you must specify a value for the **proxy** option.
- **real-http-persistence**
  Specifies whether to enable or disable real HTTP persistence. When enabled, the RTSP filter automatically persists Real Networks RTSP over HTTP using the RTSP port. The default value is **enabled**. If you disable this parameter, you can override the default behavior with an iRule.
- **regex**
  Displays the items that match the regular expression. The regular expression must be preceded by an at sign (@[regular expression]) to indicate that the identifier is a regular expression. See **help regex** for a description of regular expression syntax.
- **rtcp-port**
  Specifies the number of the port to use for the Real Time Control Protocol (RTCP) service. The default value is **0** (zero). RTCP allows monitoring of real-time data delivery.
- **rtp-port**
  Specifies the number of the port to use for the RTP service. The default value is **0** (zero).

- **session-reconnect**
  Specifies whether to enable or disable session reconnect. When enabled, the RTSP filter persists the control connection, which is being resumed, to the correct server. The default value is **disabled**.
- **to-folder**
  rtsp profiles can be moved to any folder under **/Common**, but configuration depenedencies may restrict moving the profile out of **/Common**.
- **unicast-redirect**
  Specifies whether to enable or disable unicast redirect. When enabled, the client can select the destination to which to stream data. The default value is **disabled**.
- **log-publisher**
  Specify the name of the log publisher which logs translation events. See **help sys log-config** for more details on the logging sub-system. Use the *publisher* component to set up a log publisher.
- **log-profile**
  Specify the name of the ALG log profile which controls the logging of ALG . See **help ltm alg-log-profile** for more details on the logging profile sub-system. Use the ltm alg-log-profile profile component to set up a ALG log profile.

See Also

create, *delete*, *edit*, glob, *list*, *virtual*, *modify*, *mv*, regex, *reset-stats*, *show*, *tmsh*

sctp

Configures a Stream Control Transmission Protocol (SCTP) profile.

Syntax

Configure the **sctp** component within the **ltm profile** module using the syntax shown in the following sections.

Create

```
create sctp [name]
modify sctp [name]
    app-service [[string] | none]
    cookie-expiration [integer]
    defaults-from [name]
    description [string]
    heartbeat-interval [integer]
    heartbeat-max-burst [integer]
    idle-timeout [integer]
    in-streams [integer]
    init-max-retries [integer]
    ip-tos [integer]
    link-qos [integer]
    max-burst [integer]
    out-streams [integer]
    proxy-buffer-high [integer]
    proxy-buffer-low [integer]
    receive-chunks [integer]
    receive-ordered [disabled | enabled]
    receive-window-size [integer]
    reset-on-timeout [disabled | enabled]
    secret [default | [string] ]
    send-buffer-size [integer]
    send-max-retries [integer]
    send-partial [disabled | enabled]
    tcp-shutdown [disabled | enabled]
    transmit-chunks [integer]
edit sctp [ [ [name] | [glob] | [regex] ] ... ]
    all-properties
    non-default-properties
mv sctp [ [[source-name] [destination-name]] | [[name] to-folder [folder-name]] |
[[name...name] to-folder [folder-name]] ]
    to-folder
reset-stats sctp
reset-stats sctp [ [ [name] | [glob] | [regex] ] ... ]
```

Display

```
list sctp
list sctp [ [ [name] | [glob] | [regex] ] ... ]
show running-config sctp
show running-config sctp
  [ [ [name] | [glob] | [regex] ] ... ]
    all-properties
```

```
    non-default-properties
    one-line
    partition
show sctp
show sctp [ [ [name] | [glob] | [regex] ] ... ]
    (default | exa | gig | kil | meg | peta | raw | tera | yotta | zetta)
    field-fmt
    global
```

Delete

```
delete sctp [name]
```

Description

You can use the **sctp** component to manage a profile for SCTP traffic.

Examples

create sctp my_sctp_profile defaults-from sctp

Creates a custom SCTP profile named **my_sctp_profile** that inherits its settings from the system default SCTP profile.

list sctp all-properties

Displays all properties for all SCTP profiles.

mv sctp /Common/my_sctp_profile to-folder /Common/my_folder

Moves a custom sctp profile named **my_sctp_profile** to a folder named **my_folder**, where **my_folder** has already been created and exists within **/Common**.

Options

- **app-service**
  Specifies the name of the application service to which the profile belongs. The default value is **none**. **Note:** If the **strict-updates** option is **enabled** on the application service that owns the object, you cannot modify or delete the profile. Only the application service can modify or delete the profile.
- **cookie-expiration**
  Specifies how many seconds the cookie is valid. The default value is **60** seconds.
- **defaults-from**
  Specifies the profile that you want to use as the parent profile. Your new profile inherits all settings and values from the parent profile specified. The default value is **sctp**.
- **description**
  User defined description.

- **glob**
  Displays the items that match the **glob** expression. See **help glob** for a description of **glob** expression syntax.
- **heartbeat-interval**
  Specifies the number of seconds to wait before sending a heartbeat chunk. The default value is **30** seconds.
- **heartbeat-max-burst**
  Specifies the number of heartbeat packets to be sent in a single burst. The default value is **1**.
- **idle-timeout**
  Specifies the number of seconds without traffic before a connection is eligible for deletion. The default value is **300** seconds.
- **in-streams**
  Specifies the number of inbound streams. The default value is **2**.
- **init-max-retries**
  Specifies the maximum number of retries to establish a connection. The default value is **4**.
- **ip-tos**
  Specifies the Type of Service (ToS) that is set in packets sent to the peer. The default value is **0**.
- **link-qos**
  Specifies the Link Quality of Service (QoS) that is set in sent packets. The default value is **0**.
- **name**
  Specifies a unique name for the component. This option is required for the commands **create**, **delete**, and **modify**.
- **out-streams**
  Specifies the number of outbound streams. The default value is **2**.
- **partition**
  Displays the administrative partition within which the component resides.
- **proxy-buffer-high**
  Specifies the proxy buffer level after which the system closes the receive window. The default value is **16384**.
- **proxy-buffer-low**
  Specifies the proxy buffer level after which the system opens the receive window. The default value is **4096**.
- **receive-chunks**
  Specifies the size (in chunks) of the rx_chunk buffer. The default value is **256**.
- **receive-ordered**
  When **enabled**, the default, the system delivers messages to the application layer in order.
- **receive-window-size**
  Specifies the size (in bytes) of the receive window. Prorate this value to the **receive-chunks** value. The default value is **65535**.

- **regex**
  Displays the items that match the regular expression. The regular expression must be preceded by an at sign (@[regular expression]) to indicate that the identifier is a regular expression. See **help regex** for a description of regular expression syntax.
- **reset-on-timeout**
  When **enabled**, the default, the system resets the connection when the connection times out.
- **secret**
  Specifies the internal secret string used for HTTP Message Authenticated Code (HMAC) cookies.
- **send-buffer-size**
  Specifies the size in bytes of the buffer. The default value is **65536**.
- **max-burst**
  Specifies the maximum number of data packets to send in a single burst. The default value is **4**.
- **send-max-retries**
  Specifies the maximum number of time the system tries again to send the data. The default value is **8**.
- **send-partial**
  When **enabled**, the default, the system accepts partial application data.
- **tcp-shutdown**
  When **enabled**, the system emulates the closing of a TCP connection. The default value is **enabled**.
- **to-folder**
  sctp profiles can be moved to any folder under **/Common**, but configuration depenedencies may restrict moving the profile out of **/Common**.
- **transmit-chunks**
  Specifies the size of the tx_chunk buffer. The default value is **256**.

See Also

create, *delete*, *edit*, glob, *list*, *virtual*, *modify*, *mv*, regex, *reset-stats*, *show*, *tmsh*

server-ldap

Configures an Server LDAP profile.

Syntax

Configure the **server-ldap** component within the **ltm profile** module using the syntax shown in the following sections.

Create/Modify

```
create server-ldap [name]
modify server-ldap [name]
    app-service [[string] | none]
    defaults-from [ [name] | none]
    description [string]
    activation-mode [ none | allow | require ]
    ss-activation-mode [ none | allow | require ]
edit server-ldap [ [ [name] | [glob] | [regex] ] ... ]
    all-properties
    non-default-properties
```

Display

```
list server-ldap
list server-ldap [ [ [name] | [glob] | [regex] ] ... ]
show running-config server-ldap
show running-config server-ldap [ [ [name] | [glob] | [regex] ] ... ]
    all-properties
    non-default-properties
```

Delete

```
delete server-ldap [name]
```

Description

You can use the **server-ldap** component to create, modify, display, or delete an Server LDAP profile with which you can manage Server LDAP traffic.

Examples

create server-ldap my_serverldap_profile defaults-from serverldap

Creates a custom Server LDAP profile named **my_serverldap_profile** that inherits its settings from the system default Server LDAP profile.

list server-ldap

Displays the properties of all Server LDAP profiles.

Options

- **app-service**
  Specifies the name of the application service to which the profile belongs. The default value is **none**. **Note:** If the **strict-updates** option is **enabled** on the application service that owns the object, you cannot modify or delete the profile. Only the application service can modify or delete the profile.
- **defaults-from**
  Specifies the profile that you want to use as the parent profile. Your new profile inherits all settings and values from the parent profile specified. The default value is **smtp**.
- **description**
  User defined description.
- **glob**
  Displays the items that match the **glob** expression. See **help glob** for a description of **glob** expression syntax.
- **name**
  Specifies a unique name for the component. This option is required for the commands **create**, **delete**, and **modify**.
- **regex**
  Displays the items that match the regular expression. The regular expression must be preceded by an at sign (@[regular expression]) to indicate that the identifier is a regular expression. See **help regex** for a description of regular expression syntax.
- **activation-mode**
  Sets the activation-mode for STARTTLS. The options are NONE, ALLOW, or REQUIRE. The default value is NONE.

See Also

create, *delete*, *edit*, glob, *list*, *virtual*, *modify*, regex, *reset-stats*, *show*, *provision*, *tmsh*

server-ssl

Configures a Server SSL profile.

Syntax

Configure the **server-ssl** component within the **ltm profile** module using the syntax shown in the following sections.

Create/Modify

```
create server-ssl [name]
modify server-ssl [name]
    alert-timeout [indefinite | [integer] ]
    app-service [[string] | none]
    authenticate [always | once]
    authenticate-depth [integer]
    authenticate-name [ [name] | none]
    ca-file [ [file name] | none]
    cache-size [integer]
    cache-timeout [integer]
    cert [ [file name] | none]
    chain [ [name] | none]
    ciphers [ [name] | none]
    crl-file [none]
    defaults-from [ [name] | none]
    description [string]
    expire-cert-response-control [drop | ignore]
    handshake-timeout [indefinite | [integer] ]
    key [ [file name] | none]
    mod-ssl-methods [disabled | enabled]
    mode [disabled | enabled]
    options {
      none |
      [ all-bugfixes cipher-server-preference
        dont-insert-empty-fragments ephemeral-rsa
        microsoft-big-sslv3-buffer microsoft-sess-id-bug
        msie-sslv2-rsa-padding netscape-ca-dn-bug
        netscape-challenge-bug netscape-demo-cipher-change-bug
        netscape-reuse-cipher-change-bug
        no-session-resumption-on-renegotiation
        no-ssl no-sslv2 no-sslv3 no-tls no-tlsv1 no-tlsv1.1 no-tlsv1.2
        no-dtls passive-close pkcs1-check-1
        pkcs1-check-2 single-dh-use ssleay-080-client-dh-bug
        sslref2-reuse-cert-type-bug tls-block-padding-bug tls-d5-bug
        tls-rollback-bug ]
    }
    passphrase [none | [string] ]
    peer-cert-mode [ignore | require]
    proxy-ssl [disabled | enabled]
    proxy-ssl-passthrough [disabled | enabled]
    renegotiate-period [indefinite | [integer] ]
    renegotiate-size [indefinite | [integer] ]
    renegotiation [disabled | enabled]
    retain-certificate [true | false]
    secure-renegotiation [request | require | require-strict]
    server-name [name]
```

```
    session-mirroring [disabled | enabled]
    session-ticket [disabled | enabled]
    generic-alert [disabled | enabled]
    sni-default [true | false]
    sni-require [true | false]
    ssl-forward-proxy [disabled | enabled]
    ssl-forward-proxy-bypass [disabled | enabled]
    ssl-sign-hash [any | sha1 | sha256 | sha384]
    strict-resume [disabled | enabled]
    unclean-shutdown [disabled | enabled]
    untrusted-cert-response-control [drop | ignore]
edit server-ssl [ [ [name] | [glob] | [regex] ] ... ]
    all-properties
    non-default-properties
mv server-ssl [ [[source-name] [destination-name]] | [[name] to-folder [folder-name]]
| [[name...name] to-folder [folder-name]] ]
    to-folder
reset-stats server-ssl
reset-stats server-ssl [ [ [name] | [glob] | [regex] ] ... ]
```

Display

```
list server-ssl
list server-ssl [ [ [name] | [glob] | [regex] ] ... ]
show running-config server-ssl
show running-config server-ssl
  [ [ [name] | [glob] | [regex] ] ... ]
    all-properties
    non-default-properties
    one-line
    partition
show server-ssl
show server-ssl [ [ [name] | [glob] | [regex] ] ... ]
    (default | exa | gig | kil | meg | peta | raw | tera | yotta | zetta)
    global
```

Delete

```
delete server-ssl [name]
```

Description

You can use the **server-ssl** component to manage a server SSL profile.

Server-side profiles enable the traffic management system to handle encryption tasks for any SSL connection being sent from a local traffic management system to a target server. A server-side SSL profile is acts as a client by presenting certificate credentials to a server when authentication of the local traffic management system is required. You implement this type of profile by using the default profile, or by creating a custom profile based on the Server SSL profile template and modifying its settings.

Examples

create server-ssl my_serverssl_profile defaults-from serverssl

Creates a custom Server SSL profile named **my_serverssl_profile** that inherits its settings from the system default profile **serverssl**.

list server-ssl all-properties

Displays all properties for all Server SSL profiles.

mv server-ssl /Common/my_serverssl_profile to-folder /Common/my_folder

Moves a custom server-ssl profile named **my_serverssl_profile** to a folder named **my_folder**, where **my_folder** has already been created and exists within **/Common**.

Options

- **app-service**
  Specifies the name of the application service to which the profile belongs. The default value is **none**. **Note:** If the **strict-updates** option is **enabled** on the application service that owns the object, you cannot modify or delete the profile. Only the application service can modify or delete the profile.
- **alert-timeout**
  Specifies the maximum time period in seconds to keep the SSL session active after alert message is sent. The default value is **10** seconds.
- **authenticate**
  Specifies the frequency of authentication. The default value is **once**.
- **authenticate-depth**
  Specifies the client certificate chain maximum traversal depth. The default value is **9**.
- **authenticate-name**
  Specifies a Common Name (CN) that is embedded in a server certificate. The system authenticates a server based on the specified CN. The default value is **none**.
- **ca-file**
  Specifies the certificate authority file name. Configures certificate verification by specifying a list of client or server CAs that the traffic management system trusts. The default value is **none**.
- **cache-size**
  Specifies the SSL session cache size. For client profiles only, you can configure timeout and size values for the SSL session cache. Because each profile maintains a separate SSL session cache, you can configure the values on a per-profile basis. The default value is **262144**.

- **cache-timeout**
  Specifies the SSL session cache timeout value, which is the usable lifetime seconds of negotiated SSL session IDs. The default value is **3600** seconds. Acceptable values are integers greater than or equal to **0** and less than or equal to **86400**.
- **cert**
  Specifies the name of the certificate installed on the traffic management system for the purpose of terminating or initiating an SSL connection. The default value is **none**.
- **chain**
  Specifies or builds a certificate chain file that a client can use to authenticate the profile. The default value is **none**.
- **ciphers**
  Specifies a cipher name. The default value is **DEFAULT**.
- **crl-file**
  Specifies the certificate revocation list file name. The default value is **none**.
- **defaults-from**
  Specifies the profile that you want to use as the parent profile. Your new profile inherits all settings and values from the parent profile specified. The default value is **serverssl**.
- **description**
  User defined description.
- **expire-cert-response-control**
  Specifies the BIGIP action when the server certificate has expired. The default value is **drop**, which causes the connection to be dropped. Conversely, you can specify **ignore** to cause the connection to ignore the error and continue.
- **glob**
  Displays the items that match the **glob** expression. See **help glob** for a description of **glob** expression syntax.
- **handshake-timeout**
  Specifies the handshake timeout in seconds. The default value is **10**.
- **key**
  Specifies the key file name. Specifies the name of the key installed on the traffic management system for the purpose of terminating or initiating an SSL connection. The default value is **none**.
- **mod-ssl-methods**
  Enables or disables ModSSL methods. The default value is **disabled**. Enable this option when OpenSSL methods are inadequate. For example, you can enable ModSSL method emulation when you want to use SSL compression over TLSv1.
- **mode**
  Enables or disables SSL processing. The default value is **enabled**.
- **name**
  Specifies a unique name for the component. This option is required for the commands **create**, **delete**, and **modify**.

- **options**
  Enables options, including some industry-related workarounds. Enter options inside braces, for example, **{ dont-insert-empty-fragments microsoft-sess-id-bug}**. The default value is **dont-insert-empty-fragments**.
  - **all-bugfixes**
    This option enables the following industry-related defect workarounds: microsoft-sess-id-bug, netscape-challenge-bug, netscape-reuse-cipher-change-bug, sslref2-reuse-cert-type-bug, microsoft-big-sslv3-buffer, msie-sslv2-rsa-padding, ssleay-080-client-dh-bug, tls-d5-bug, tls-block-padding-bug, and dont-insert-empty-fragments.
    It is usually safe to use this option to enable the defect workaround options when compatibility with broken implementations is desired. Note that if you edit the configuration in the browser-based Configuration utility, the system expands the **all-bugfixes** syntax into each individual option.
  - **cipher-server-preference**
    When choosing a cipher, this option uses the server's preferences instead of the client references. When this option is not set, the SSL server always follows the client's references. When this option is set, the SSLv3/TLSv1 server chooses by using its own references. Due to the different protocol, for SSLv2 the server sends its list of preferences to the client and the client always chooses.
  - **dont-insert-empty-fragments**
    Disables a countermeasure against a SSL 3.0/TLS 1.0 protocol vulnerability affecting CBC ciphers. These ciphers cannot be handled by certain broken SSL implementations. This option has no effect for connections using other ciphers.
  - **ephemeral-rsa**
    Uses ephemeral (temporary) RSA keys when doing RSA operations. According to the specifications, this is only done when an RSA key can be used for signature operations (namely under export ciphers with restricted RSA key length). By setting this option, you specify that you always want to use ephemeral RSA keys. This option breaks compatibility with the SSL/TLS specifications and may lead to interoperability problems with clients. Therefore, F5 Networks does not recommend this option. Use ciphers with EDH (ephemeral Diffie-Hellman) key exchange instead. This option is ignored for server-side SSL.
  - **microsoft-big-sslv3-buffer**
    Enables a workaround for communicating with older Microsoft® applications that use non-standard SSL record sizes.
  - **microsoft-sess-id-bug**
    Handles a Microsoft session ID problem.
  - **msie-sslv2-rsa-padding**
    Enables a workaround for communicating with older Microsoft applications that use non-standard RSA key padding. This option is ignored for server-side SSL.

- **netscape-ca-dn-bug**
  Handles a defect regarding the system crashing or hanging. If the system accepts a Netscape Navigator® browser connection, demands a client cert, has a non-self-signed CA that does not have its CA in Netscape, and the browser has a certificate, the system crashes or hangs.
- **netscape-challenge-bug**
  Handles the Netscape challenge problem.
- **netscape-demo-cipher-change-bug**
  Manipulates the SSL server session resumption behavior to mimic that of certain Netscape servers (see the Netscape reuse cipher change bug workaround description). Note that F5 Networks does not recommend this option for normal use. It is ignored for server-side SSL.
- **netschape-reuse-cipher-change-bug**
  Handles a defect within Netscape-Enterprise/2.01 (https://merchant.neape.com), appearing only when connecting through SSLv2/v3, and then reconnecting through SSLv3. In this case, the cipher list changes.
  First, a connection is established with the RC4-MD5 cipher list. If it is then resumed, the connection switches to using the DES-CBC3-SHA cipher list. However, according to RFC 2246, (section 7.4.1.3, cipher suite) the cipher list is RC4-MD5.
  As a workaround, you can attempt to connect with a cipher list of DES-CBC-SHA:RC4-MD5 and so on. For some reason, each new connection uses the RC4-MD5 cipher list, but any re-connection attempts to use the DES-CBC-SHA cipher list. Thus Netscape, when reconnecting, always uses the first cipher in the cipher list.
- **no-session-resumption-on-renegotiation**
  When performing renegotiation as an SSL server, this option always starts a new session (that is, session resumption requests are accepted only in the initial handshake). The system ignores this option for server-side SSL.
- **no-ssl**
  Do not use any version of the SSL protocol.
- **no-sslv2**
  Do not use the SSLv2 protocol.
- **no-sslv3**
  Do not use the SSLv3 protocol.
- **no-tls**
  Do not use any version of the TLS protocol.
- **no-tlsv1**
  Do not use the TLSv1.0 protocol.
- **no-tlsv1.1**
  Do not use the TLSv1.1 protocol.
- **no-tlsv1.2**
  Do not use the TLSv1.2 protocol.

- **no-dtls**
  Do not use any version of the DTLS protocol.
- **passive-close**
  Specifies how to handle passive closes.
- **none**
  Disables all workarounds. Note that F5 Networks does not recommend this option.
- **pkcs1-check-1**
  This debugging option deliberately manipulates the PKCS1 padding used by SSL clients in an attempt to detect vulnerability to particular SSL server vulnerabilities. Note that F5 Networks does not recommend this option for normal use. The system ignores this option for client-side SSL.
- **pkcs1-check-2**
  This debugging option deliberately manipulates the PKCS1 padding used by SSL clients in an attempt to detect vulnerability to particular SSL server vulnerabilities. Note that F5 Networks does not recommend this option for normal use. The system ignores this option for client-side SSL.
- **single-dh-use**
  Creates a new key when using temporary/ephemeral DH parameters. This option must be used to prevent small subgroup attacks, when the DH parameters were not generated using strong primes (for example. when using DSA-parameters). If strong primes were used, it is not strictly necessary to generate a new DH key during each handshake, but F5 Networks recommends it. Enable the Single DH Use option whenever temporary or ephemeral DH parameters are used.
- **ssleay-080-client-dh-bug**
  Enables a workaround for communicating with older SSLeay-based applications that specify an incorrect Diffie-Hellman public value length. This option is ignored for server-side SSL.
- **sslref2-reuse-cert-type-bug**
  Handles the SSL reuse certificate type problem.
- **tls-block-padding-bug**
  Enables a workaround for communicating with older TLSv1-enabled applications that use incorrect block padding.
- **tls-d5-bug**
  This option is a workaround for communicating with older TLSv1-enabled applications that specify an incorrect encrypted RSA key length. This option is ignored for server-side SSL.
- **tls-rollback-bug**
  Disables version rollback attack detection. During the client key exchange, the client must send the same information about acceptable SSL/TLS protocol levels as it sends during the first hello. Some clients violate this rule by adapting to the server's answer. For example, the client sends an SSLv2 hello and accepts up to SSLv3.1 (TLSv1), but the server only processes up to SSLv3. In this case, the client must still use the same SSLv3.1 (TLSv1) announcement. Some

clients step down to SSLv3 with respect to the server's answer and violate the version rollback protection. The system ignores this option for server-side SSL.

- **partition**
  Displays the administrative partition within which the component resides.
- **passphrase**
  Specifies the key passphrase, if required. The default value is **none**.
- **peer-cert-mode**
  Specifies the peer certificate mode. The default value is **ignore**.
- **proxy-ssl**
  Enabling this option requires a corresponding client ssl profile with **proxy-ssl** enabled to perform transparent SSL decryption. This feature allows further modification of application traffic within an SSL tunnel while still allowing the server to perform necessary authorization, authentication, auditing steps.
- **proxy-ssl-passthrough**
  Enabling this option requires a corresponding client ssl profile with **proxy-ssl-passthrough** enabled. This allows Proxy SSL to passthrough the traffic when ciphersuite negotiated between the client and server is not supported. The default option is **disabled**.
- **regex**
  Displays the items that match the regular expression. The regular expression must be preceded by an at sign (@[regular expression]) to indicate that the identifier is a regular expression. See **help regex** for a description of regular expression syntax.
- **renegotiate-period**
  Specifies the number of seconds from the initial connect time after which the system renegotiates an SSL session. The default value is **indefinite**, which means that you do not want the system to renegotiate SSL sessions.
  Each time the session renegotiation is successful, a new connection is started. Therefore, the system attempts to renegotiate the session again, in the specified amount of time following a successful session renegotiation. For example, setting the **renegotiate-period** option to **3600** seconds triggers session renegotiation at least once an hour.
- **renegotiate-size**
  Specifies a throughput size, in megabytes, of SSL renegotiation. This option forces the traffic management system to renegotiate an SSL session based on the size, in megabytes, of application data that is transmitted over the secure channel. The default value is **indefinite**, which specifies that you do not want a throughput size.
- **renegotiation**
  Specifies whether renegotiations are enabled. The default value is **enabled**. When renegotiations are disabled, the system is acting as an SSL server, and a COMPAT or NATIVE cipher is negotiated, the system

will abort the connection. Additionally, when renegotiations are disabled and the system is acting as an SSL client, the system will ignore the server's HelloRequest messages.

- **retain-certificate**
  APM module requires storing certificate in SSL session. When set to false, certificate will not be stored in SSL session. The default value is **true**.
- **generic-alert**
  Enables or disables generic-alert. The default option is **enabled**, which causes the SSL profile to use generic alert number. Conversely, you can specify **disabled** to cause SSL profile to use alert number defined in RFC5246/RFC6066 strictly.
- **secure-renegotiation**
  Specifies the secure renegotiation mode. The default value is **require-strict**. When secure renegotiation is set to **require**, any connection to an unpatched server will be aborted. For server-ssl, there is no difference between **require** and **require-strict** secure renegotiation. When secure renegotiation is set to **request**, connections to unpatched servers will be permitted. This setting is NOT recommended however, as it is subject to active man-in-the-middle attacks.
- **server-name**
  Specifies the server name to be included in SNI (server name indication) extension during SSL handshake in ClientHello.
- **session-mirroring**
  Enables or disables the mirroring of sessions to high availability peer. By default, this setting is disabled, which causes the system to not mirror ssl sessions.
- **session-ticket**
  Enables or disables session-ticket. The default option is **disabled**, which causes the SSL profile not to use session ticket per RFC 5077. Conversely, you can specify **enabled** to cause SSL profile to use session ticket per RFC 5077.
- **sni-default**
  When true, this profile is the default SSL profile when the server name in a client connection does not match any configured server names, or a client connection does not specify any server name at all.
- **sni-require**
  When this option is enabled, connections to a server that does not support SNI extension will be rejected.
- **ssl-forward-proxy**
  Enables or disables ssl-forward-proxy feature. The default option is **disabled**. Conversely, you can specify **enabled** to use the SSL Forward Proxy Feature.
- **ssl-sign-hash**
  Specifies SSL sign hash algorithm which is used to sign and verify SSL Server Key Exchange and Certificate Verify messages for the specified SSL profiles. The default value is **sha1**.

- **ssl-forward-proxy-bypass**
  Enables or disables ssl-forward-proxy-bypass feature. The default option is **disabled**. Conversely, you can specify **enabled** to use the SSL Forward Proxy Bypass Feature.
- **strict-resume**
  Enables or disables the resumption of SSL sessions after an unclean shutdown. The default value is **disabled**, which indicates that the SSL profile refuses to resume SSL sessions after an unclean shutdown.
- **to-folder**
  server-ssl profiles can be moved to any folder under **/Common**, but configuration dependencies may restrict moving the profile out of **/Common**.
- **unclean-shutdown**
  Specifies, when enabled, that the SSL profile performs unclean shutdowns of all SSL connections, which means that underlying TCP connections are closed without exchanging the required SSL shutdown alerts. If you want to force the SSL profile to perform a clean shutdown of all SSL connections, you can disable this option.
- **untrusted-cert-response-control**
  Specifies the BIGIP action when the server certificate has untrusted CA. The default value is **drop**, which causes the connection to be dropped. Conversely, you can specify **ignore** to cause the connection to ignore the error and continue.

See Also

create, *delete*, *edit*, glob, *list*, *client-ssl*, *virtual*, *modify*, *mv*, regex, *show*, *tmsh*

sip

Configures a Session Initiation Protocol (SIP) profile.

Syntax

Configure the **sip** component within the **ltm profile** module using the syntax shown in the following sections.

Create/Modify

```
create sip [name]
modify sip [name]
    alg-enable [disabled | enabled]
    app-service [[string] | none]
    community [ [community name] | none]
    defaults-from [ [name] | none]
    description [string]
    dialog-aware [disabled | enabled]
    dialog-establishment-timeout [integer]
    enable-sip-firewall [no | yes]
    insert-record-route-header [disabled | enabled]
    insert-via-header [disabled | enabled]
    max-media-sessions [integer]
    max-registrations [integer]
    max-sessions-per-registration [integer]
    max-size [integer]
    registration-timeout [integer]
    rtp-proxy-style [symmetric | restricted-by-ip-address | any-location]
    secure-via-header [disabled | enabled]
    security [disabled | enabled]
    sip-session-timeout [integer]
    terminate-on-bye [disabled | enabled]
    user-via-header [ [via-header] | none]
    log-publisher [log publisher name | none]
    log-profile [log profile name | none]
edit sip [ [ [name] | [glob] | [regex] ] ... ]
    all-properties
    non-default-properties
mv sip [ [[source-name] [destination-name]] | [[name] to-folder [folder-name]] |
[[name...name] to-folder [folder-name]] ]
    to-folder
reset-stats sip
reset-stats sip [ [ [name] | [glob] | [regex] ] ... ]
```

Display

```
list sip
list sip [ [ [name] | [glob] | [regex] ] ... ]
show running-config sip
show running-config sip [ [ [name] | [glob] | [regex] ] ... ]
    all-properties
    non-default-properties
    one-line
    partition
```

```
show sip
show sip [ [ [name] | [glob] | [regex] ] ... ]
    (default | exa | gig | kil | meg | peta | raw | tera | yotta | zetta)
    field-fmt
```

Delete

```
delete sip [name]
```

Description

You can use the **sip** component to manage a SIP profile.

Examples

create sip my_sip_profile defaults-from sip

Creates a SIP profile named **my_sip_profile** using the system defaults.

create sip my_sip_profile { terminate-bye disabled }

Creates a SIP profile named **my_sip_profile** that leaves a connection open following the completion of a BYE transaction.

mv sip /Common/my_sip_profile to-folder /Common/my_folder

Moves a custom sip profile named **my_sip_profile** to a folder named **my_folder**, where **my_folder** has already been created and exists within **/Common**.

Options

- **alg-enable**
  Enables or disables the SIP ALG (Application Level Gateway) feature. The default value is **disabled**. **Note:** for a SIP profile with ALG enabled to function correctly, the **virtual** which uses the profile must have **destination** and **mask** set to **0.0.0.0** for IPv4, or **::** for IPv6. Additionally, the **virtual** must have **source-address-translation** enabled.
- **app-service**
  Specifies the name of the application service to which the object belongs. The default value is **none**. **Note:** If the **strict-updates** option is **enabled** on the application service that owns the object, you cannot modify or delete the object. Only the application service can modify or delete the object.
- **community**
  Specifies the community to which you want to assign the virtual server that you associate with this profile. The default value is **none**.
- **defaults-from**
  Specifies the profile that you want to use as the parent profile. Your new profile inherits all of the settings and values from the specified parent profile. The default value is **sip**.

- **description**
  User defined description.
- **dialog-aware**
  Enables or disables the ability for the system to be aware of unauthorized use of the SIP dialog. The default value is **disabled**.
- **dialog-establishment-timeout**
  Indicates the timeout value for dialog establishment in a sip session. The default value is **10** seconds.
- **enable-sip-firewall**
  Indicates whether to enable SIP firewall functionality or not. Default value is **no**.
- **glob**
  Displays the items that match the **glob** expression. See **help glob** for a description of **glob** expression syntax.
- **insert-record-route-header**
  Enables or disables the insertion of a Record-Route header, which indicates the next hop for the following SIP request messages. The default value is **disabled**.
- **insert-via-header**
  Enables or disables the insertion of a Via header, which indicates where the message originated. The response message uses this routing information. The default value is **disabled**.
- **max-media-sessions**
  Indicates the maximum number of SDP media sessions that the BIG-IP system accepts. The default value is **6**.
- **max-registrations**
  Indicates the maximum number of registrations, the maximum allowable REGISTER messages can be recorded that the BIG-IP system accepts. The default value is **100**.
- **max-sessions-per-registration**
  Indicates the maximum number of calls or sessions can be made by a user for a single registration that the BIG-IP system accepts. The default value is **50**.
- **max-size**
  Specifies the maximum SIP message size that the BIG-IP system accepts. The default value is **65535** bytes.
- **name**
  Specifies a unique name for the component. This option is required for the commands **create**, **delete**, and **modify**.
- **partition**
  Displays the administrative partition within which the component resides.
- **regex**
  Displays the items that match the regular expression. The regular expression must be preceded by an at sign (@[regular expression]) to indicate that the identifier is a regular expression. See **help regex** for a description of regular expression syntax.

- **registration-timeout**
  Indicates the timeout value for a sip registration. The default value is **3600** seconds.
- **rtp-proxy-style**
  Indicates the style in which the RTP will proxy the data. When a dialog is established, the necessary SDP data needs to know where the RTP flows are directed. The default value is **symmetric**. The options available are:
  - **symmetric**
    Indicates the use of a bidirectional related flow.
  - **restricted-by-ip-address**
    Indicates the use of ephemeral listeners to support fixed client IP, listener is restricted to connections coming from a particular source.
  - **any-location**
    Indicates the use of ephemeral listeners to support wildcard, connections are allowed to come from anyway.
- **secure-via-header**
  Enables or disables the insertion of a Secure Via header, which indicates where the message originated. When you are using SSL/TLS (over TCP) to create a secure channel with the server node, use this setting to configure the system to insert a Secure Via header into SIP requests. The default value is **disabled**.
- **security**
  Enables or disables security for the SIP profile. The default value is **disabled**.
- **sip-session-timeout**
  Indicates the timeout value for a sip session. The default value is **300** seconds.
- **terminate-on-bye**
  Enables or disables the termination of a connection when a BYE transaction finishes. Use this parameter with UDP connections only, not with TCP connections. The default value is **enabled**.
- **to-folder**
  sip profiles can be moved to any folder under **/Common**, but configuration dependencies may restrict moving the profile out of **/Common**.
- **user-via-header**
  Enables or disables the insertion of a Via header specified by a system administrator. The default value is **none**.
- **log-publisher**
  Specify the name of the log publisher which logs translation events. See **help sys log-config** for more details on the logging sub-system. Use the *publisher* component to set up a log publisher.
- **log-profile**
  Specify the name of the ALG log profile which controls the logging of ALG . See **help ltm alg-log-profile** for more details on the logging profile sub-system. Use the ltm alg-log-profile profile component to set up a ALG log profile.

See Also

create, *delete*, *edit*, glob, *list*, *virtual*, *modify*, *mv*, regex, *reset-stats*, *show*, *tmsh*

smtp

Configures an SMTP profile.

Syntax

Configure the **smtp** component within the **ltm profile** module using the syntax shown in the following sections. The **smtp** profile is available when the **asm** module is enabled. You enable the asm module via provisioning commands, which are described in **help sys provision**.

Create/Modify

```
create smtp [name]
modify smtp [name]
    app-service [[string] | none]
    defaults-from [ [name] | none]
    description [string]
    security [disabled | enabled]
edit smtp [ [ [name] | [glob] | [regex] ] ... ]
    all-properties
    non-default-properties
```

Display

```
list smtp
list smtp [ [ [name] | [glob] | [regex] ] ... ]
show running-config smtp
show running-config smtp [ [ [name] | [glob] | [regex] ] ... ]
    all-properties
    non-default-properties
```

Delete

```
delete smtp [name]
```

Description

You can use the **smtp** component to create, modify, display, or delete an SMTP profile with which you can manage SMTP traffic.

Examples

create smtp my_smtp_profile defaults-from smtp

Creates a custom SMTP profile named **my_smtp_profile** that inherits its settings from the system default SMTP profile.

list smtp

Displays the properties of all SMTP profiles.

Options

- **app-service**
  Specifies the name of the application service to which the profile belongs. The default value is **none**. **Note:** If the **strict-updates** option is **enabled** on the application service that owns the object, you cannot modify or delete the profile. Only the application service can modify or delete the profile.
- **defaults-from**
  Specifies the profile that you want to use as the parent profile. Your new profile inherits all settings and values from the parent profile specified. The default value is **smtp**.
- **description**
  User defined description.
- **glob**
  Displays the items that match the **glob** expression. See **help glob** for a description of **glob** expression syntax.
- **name**
  Specifies a unique name for the component. This option is required for the commands **create**, **delete**, and **modify**.
- **regex**
  Displays the items that match the regular expression. The regular expression must be preceded by an at sign (@[regular expression]) to indicate that the identifier is a regular expression. See **help regex** for a description of regular expression syntax.
- **security**
  Enables or disables secure SMTP traffic for the BIG-IP® Application Security Manager. The default value is **disabled**.

See Also

create, *delete*, *edit*, glob, *list*, *virtual*, *modify*, regex, *reset-stats*, *show*, *provision*, *tmsh*

smtps

Configures an SMTPs profile.

Syntax

Configure the **smtps** component within the **ltm profile** module using the syntax shown in the following sections. The **smtps** profile is available when the **asm** module is enabled. You enable the asm module via provisioning commands, which are described in **help sys provision**.

Create/Modify

```
create smtps [name]
modify smtps [name]
    app-service [[string] | none]
    defaults-from [ [name] | none]
    description [string]
    activation-mode [ none | allow | require ]
edit smtps [ [ [name] | [glob] | [regex] ] ... ]
    all-properties
    non-default-properties
```

Display

```
list smtps
list smtps [ [ [name] | [glob] | [regex] ] ... ]
show running-config smtps
show running-config smtps [ [ [name] | [glob] | [regex] ] ... ]
    all-properties
    non-default-properties
```

Delete

```
delete smtps [name]
```

Description

You can use the **smtps** component to create, modify, display, or delete an SMTPs profile with which you can manage SMTPs traffic.

Examples

create smtps my_smtps_profile defaults-from smtps

Creates a custom SMTPs profile named **my_smtps_profile** that inherits its settings from the system default SMTPs profile.

list smtps

Displays the properties of all SMTPs profiles.

Options

- **app-service**
  Specifies the name of the application service to which the profile belongs. The default value is **none**. **Note:** If the **strict-updates** option is **enabled** on the application service that owns the object, you cannot modify or delete the profile. Only the application service can modify or delete the profile.
- **defaults-from**
  Specifies the profile that you want to use as the parent profile. Your new profile inherits all settings and values from the parent profile specified. The default value is **smtp**.
- **description**
  User defined description.
- **glob**
  Displays the items that match the **glob** expression. See **help glob** for a description of **glob** expression syntax.
- **name**
  Specifies a unique name for the component. This option is required for the commands **create**, **delete**, and **modify**.
- **regex**
  Displays the items that match the regular expression. The regular expression must be preceded by an at sign (@[regular expression]) to indicate that the identifier is a regular expression. See **help regex** for a description of regular expression syntax.
- **activation-mode**
  Sets the activation-mode for STARTTLS. The options are NONE, ALLOW, or REQUIRE. The default value is NONE.

See Also

create, *delete*, *edit*, glob, *list*, *virtual*, *modify*, regex, *reset-stats*, *show*, *provision*, *tmsh*

socks

Configures a SOCKS profile.

Syntax

Configure the **socks** component within the **ltm profile** module using the syntax shown in the following sections.

Create/Modify

```
create socks [name]
modify socks [name]
    protocol-versions {
      [ [socks4] | [socks4a] | [socks5] ] ... ]
    }
    dns-resolver [dns-resolver]
    tunnel-name [tunnel]
    route-domain [route-domain]
    default-connect-handling [deny | allow]
edit socks [ [ [name] | [glob] | [regex] ] ... ]
    all-properties
    non-default-properties
reset-stats socks
reset-stats socks [ [ [name] | [glob] | [regex] ] ... ]
```

Display

```
list socks
list socks [ [ [name] | [glob] | [regex] ] ... ]
show running-config socks
show running-config socks [ [ [name] | [glob] | [regex] ] ... ]
    all-properties
    non-default-properties
    one-line
    partition
show socks
show socks [ [ [name] | [glob] | [regex] ] ... ]
     (default | exa | gig | kil | meg | peta | raw | tera | yotta | zetta)
     field-fmt
     global
```

Delete

```
delete socks [name]
```

Description

You can use the **socks** component to create, modify, display, or delete an SOCKS profile.

The BIG-IP® system installation includes the following default SOCKS-type profiles:

- **socks**

The default SOCKS profile contains values for properties related to managing SOCKS traffic.

You can create a new SOCKS-type profile using an existing profile as a parent profile, and then you can change the values of the properties to suit your needs.

Examples

create socks my_socks_profile defaults-from socks

Creates a custom SOCKS profile named **my_socks_profile** that inherits its settings from the system default SOCKS profile.

Options

- **protocols-versions**
  Specifies the SOCKS protocol versions that are supported. The value is one or more off:
  - **socks4**
    Specifies protocol support for SOCKS version 4.
  - **socks4a**
    Specifies protocol support for SOCKS version 4A (like version 4, but with hostname support).
  - **socks5**
    Specifies protocol support for SOCKS version 5 (with hostname and IPv6 support).

  The default value specifies all available protocols.
- **dns-resolver**
  Specifies the dns-resolver object that will be used to resolve hostnames in connect requests. The default is **dns-resolver**.
- **tunnel-name**
  Specifies the tunnel that will be used for outbound connect requests. This enables other virtual servers to receive connections initiated by the proxy service. The default is **socks-tunnel**.
- **route-domain**
  Specifies the route-domain that will be used for outbound connect requests. The default is **0**.
- **default-connect-handling**
  Specifies the behavior of the proxy service for connect requests. If set to **deny**, connect requests will only be honored if there is another virtual

server listening for the requested outbound connection. If set to **allow** outbound connections will be made regardless of other virtual servers. The default is **deny**.

See Also

create, *delete*, *edit*, glob, *list*, *virtual*, *net dns-resolver*, *route-domain*, *net tunnels*, *modify*, regex, *reset-stats*, *show*, *tmsh*

spdy

Configures a SPDY protocol profile.

Syntax

Configure the **spdy** component within the **ltm profile** module using the syntax shown in the following sections.

Create/Modify

```
create spdy [name]
modify spdy [name]
    activation-mode [npn | always]
    concurrent-streams-per-connection [integer]
    connection-idle-timeout [integer]
    defaults-from [ [name] | none]
    description [string]
    frame-size [integer]
    insert-header [disabled | enabled]
    insert-header-name ["string"]
    priority-handling [strict | fair]
    protocol-versions { [spdy3 | spdy2 | http1.1] ... }
    receive-window [integer]
    write-size [integer]
    compression-window-size [integer]
    compression-level [integer]
mv spdy [ [[source-name] [destination-name]] | [[name] to-folder [folder-name]] |
[[name...name] to-folder [folder-name]] ]
    to-folder
```

Display

```
list spdy
list spdy [ [ [name] | [glob] | [regex] ] ... ]
show running-config spdy
show running-config spdy [ [ [name] | [glob] | [regex] ] ... ]
    all-properties
    non-default-properties
    one-line
    partition
show spdy
show spdy [ [ [name] | [glob] | [regex] ] ... ]
    (default | exa | gig | kil | meg | peta | raw | tera | yotta | zetta)
    field-fmt
    global
```

Delete

```
delete spdy [name]
```

Description

You can use the **spdy** component to create, modify, display, or delete a SPDY profile.

The BIG-IP® system installation includes the following default SPDY-type profiles:

- **spdy**

The default SPDY profile contains values for properties related to managing SPDY traffic.

You can create a new SPDY-type profile using an existing profile as a parent profile, and then you can change the values of the properties to suit your needs.

Examples

create spdy my_spdy_profile defaults-from spdy

mv spdy /Common/my_spdy_profile to-folder /Common/my_folder

Moves a custom spdy profile named **my_spdy_profile** to a folder named **my_folder**, where **my_folder** has already been created and exists within **/Common**.

Options

- **activation-mode**
  Specifies what will cause a connection to be treated as a SPDY connection. The value **npn** specifies that the TLS next-protocol-negotiation will be used to determine whether SPDY should be activated. Clients that use TLS, but only support HTTP will work as-if SPDY is not present. The value **always** specifies that all connections are assumed to be SPDY connections. Clients that only support HTTP will not be able to send requests. The default value is **npn**.
- **concurrent-streams-per-connection**
  Specifies how many concurrent requests are allowed to be outstanding on a single SPDY connection.
- **connection-idle-timeout**
  Specifies how many seconds a SPDY connection is left open idly before it is shutdown.
- **defaults-from**
  Specifies the profile that you want to use as the parent profile. Your new profile inherits all settings and values from the parent profile specified. The default value is **spdy**.
- **description**
  User defined description.

- **frame-size**
  Specifies the size of the data frames, in bytes, that SPDY will send to the client. Larger frame sizes will improve network utilization, but may affect concurrency. The default value is **2048**.
- **glob**
  Displays the items that match the **glob** expression. See **help glob** for a description of **glob** expression syntax.
- **insert-header**
  Specifies whether an HTTP header that indicates the use of SPDY should be inserted in the request going to the back-end server. The default value is **disabled**.
- **insert-header-name**
  Specifies the name of the HTTP header controlled by **insert-header**. The default value is **"X-SPDY"**.
- **protocol-versions**
  Specifies which SPDY protocols clients are allowed to use. This parameter has effect with **activation-mode npn** only. Choices are **spdy3**, **spdy2**, **http1.1**. The order of the protocols is most preferred first, least preferred last. Putting **http1.1** in the list will cause SPDY to let HTTP1.1 traffic pass, if **http1.1** is not in the list, clients that don't support **http1.1** will be blocked. The client will typically pick the first protocol it supports. At least one SPDY version must be present in the list. The default value is **{ spdy3 spdy2 http1.1 }**
- **name**
  Specifies a unique name for the component. This option is required for the commands **create**, **delete**, and **modify**.
- **priority-handling**
  Specifies how SPDY should handle priorities of concurrent streams within the same connection. The value **strict** means that higher priority streams will be processed to completion before lower priority streams are processed. The value **fair** lets higher priority streams use more bandwith than lower priority stream, without completely blocking the lower priority streams. The default value is **strict**.
- **receive-window**
  Specifies the receive window, in KB. The receive window is a mechanism used by SPDY to perform flow control. The receive window allows SPDY to stall individual upload streams when needed. This mechanism is available only for SPDY version 3. The default value is **32**.
- **regex**
  Displays the items that match the regular expression. The regular expression must be preceded by an at sign (@[regular expression]) to indicate that the identifier is a regular expression. See **help regex** for a description of regular expression syntax.
- **to-folder**
  spdy profiles can be moved to any folder under **/Common**, but configuration dependencies may restrict moving the profile out of **/Common**.

- **write-size**
  Specifies the total size of combined data frames, in bytes, SPDY will send in a single write. This controls the size of the TLS records when SPDY is used over SSL. A large write size will cause SPDY to buffer more data, but will improve network utilization. The default value is **16384**.
- **compression-window-size**
  Specifies the size of the compression window, in KB. The SPDY protocol compresses http headers to save bandwidth. A larger window will allow better compression, at the cost of more memory usage. The default value is **8**.
- **compression-level**
  Specifies the level of compression used by default. This ranges from 0-10, with 10 being the most compression. Excess CPU usage will lower the level actually used to try to increase throughput. If the level is zero, then no compression is used. The default value is **5**.

See Also

create, *delete*, *edit*, glob, *list*, *fasthttp*, *virtual*, *modify*, *mv*, regex, *reset-stats*, *show*, *tmsh*

statistics

Configures a Statistics profile.

Syntax

Configure the **statistics** component within the **ltm profile** module using the syntax shown in the following sections.

Create/Modify

```
create statistics [name]
modify statistics [name]
    app-service [[string] | none]
    defaults-from [ [name] | none]
    description [string]
    field1 [string]
    field2 [string]
    field3 [string]
    field4 [string]
    field5 [string]
    field6 [string]
    field7 [string]
    field8 [string]
    field9 [string]
    field10 [string]
    field11 [string]
    field12 [string]
    field13 [string]
    field14 [string]
    field15 [string]
    field16 [string]
    field17 [string]
    field18 [string]
    field19 [string]
    field20 [string]
    field21 [string]
    field22 [string]
    field23 [string]
    field24 [string]
    field25 [string]
    field26 [string]
    field27 [string]
    field28 [string]
    field29 [string]
    field30 [string]
    field31 [string]
    field32 [string]
edit statistics [ [ [name] | [glob] | [regex] ] ... ]
    all-properties
    non-default-properties
mv statistics [ [[source-name] [destination-name]] | [[name] to-folder [folder-name]]
| [[name...name] to-folder [folder-name]] ]
    to-folder
reset-stats statistics
reset-stats statistics [ [ [name] | [glob] | [regex] ] ... ]
```

Display

```
list statistics
list statistics [ [ [name] | [glob] | [regex] ] ... ]
show running-config statistics
show running-config statistics
  [ [ [name] | [glob] | [regex] ] ... ]
    all-properties
    non-default-properties
    one-line
    partition
show statistics
show statistics [ [ [name] | [glob] | [regex] ] ... ]
    (default | exa | gig | kil | meg | peta | raw | tera | yotta | zetta)
    field-fmt
```

Delete

```
delete statistics [all | name]
```

Description

You can use the **statistics** component to create, modify, display, or delete a Statistics profile that provides user-defined statistical counters.

Examples

create statistics my_stats_profile defaults-from stats

Creates a Statistics profile name **my_stats_profile** that inherits all settings and values from the profile **stats**.

list statistics my_stats

Displays the configuration of the profile **my_stats**.

list statistics my_stats field1 total_users field2 current_users field3 max_users

Creates a Statistics profile named **my_stats** with a total users counter in Field 1 and a current users counter in Field 2. You can then write an iRule to count the total number of connections, and record the current number of connections.

For more information about writing and using iRules®, see the F5 Networks DevCentral web site at http://devcentral.f5.com.

mv statistics /Common/my_statistics_profile to-folder /Common/my_folder

Moves a custom statistics profile named **my_statistics_profile** to a folder named **my_folder**, where **my_folder** has already been created and exists within **/Common**.

Options

- **app-service**
  Specifies the name of the application service to which the profile belongs. The default value is **none**. **Note:** If the **strict-updates** option is **enabled** on the application service that owns the object, you cannot modify or delete the profile. Only the application service can modify or delete the profile.
- **defaults-from**
  Specifies the profile that you want to use as the parent profile. Your new profile inherits all settings and values from the parent profile specified. The default value is **stats**.
- **description**
  User defined description.
- **field1 ... field32**
  Specifies the name of a counter. You can specify a counter for up to 32 fields. The default value for each field is **none**.
  You can then write an iRule that uses the counter names to gather statistics about the traffic the system is processing.
- **glob**
  Displays the items that match the **glob** expression. See **help glob** for a description of **glob** expression syntax.
- **name**
  Specifies a unique name for the component. This option is required for the commands **create**, **delete**, and **modify**.
- **partition**
  Displays the administrative partition within which the component resides.
- **to-folder**
  statistics profiles can be moved to any folder under **/Common**, but configuration dependencies may restrict moving the profile out of **/Common**.
- **regex**
  Displays the items that match the regular expression. The regular expression must be preceded by an at sign (@[regular expression]) to indicate that the identifier is a regular expression. See **help regex** for a description of regular expression syntax.

See Also

create, *delete*, *edit*, glob, *list*, *modify*, *mv*, regex, *show*, *tmsh*

stream

Configures a Stream profile.

Syntax

Configure the **stream** component within the **ltm profile** module using the syntax shown in the following sections.

Create/Modify

```
create stream [name]
modify stream [name]
    app-service [[string] | none]
    defaults-from [ [name] | none]
    description [string]
    source [none | [string] ]
    target [none | [string] ]
edit stream [ [ [name] | [glob] | [regex] ] ... ]
    all-properties
    non-default-properties
mv stream [ [[source-name] [destination-name]] | [[name] to-folder [folder-name]] |
[[name...name] to-folder [folder-name]] ]
    to-folder
reset-stats stream
reset-stats stream [ [ [name] | [glob] | [regex] ] ... ]
```

Display

```
list stream
list stream [ [ [name] | [glob] | [regex] ] ... ]
show running-config stream
show running-config stream
  [ [ [name] | [glob] | [regex] ] ... ]
    all-properties
    non-default-properties
    one-line
    partition
show stream
show stream [ [ [name] | [glob] | [regex] ] ... ]
    (default | exa | gig | kil | meg | peta | raw | tera | yotta | zetta)
    field-fmt
    global
```

Delete

```
delete stream [name]
```

Description

You can use the **stream** component to search and replace strings within a data stream, such as a TCP connection.

Examples

create stream my_stream_profile defaults-from stream

Creates a custom Stream profile named **my_stream_profile** that inherits its settings from the system default **stream** profile.

list stream all-properties

Displays all properties for all Stream profiles.

mv stream /Common/my_stream_profile to-folder /Common/my_folder

Moves a custom stream profile named **my_stream_profile** to a folder named **my_folder**, where **my_folder** has already been created and exists within **/Common**.

Options

- **app-service**
  Specifies the name of the application service to which the profile belongs. The default value is **none**. **Note:** If the **strict-updates** option is **enabled** on the application service that owns the object, you cannot modify or delete the profile. Only the application service can modify or delete the profile.
- **defaults-from**
  Specifies the profile that you want to use as the parent profile. Your new profile inherits all settings and values from the parent profile specified. The default value is **stream**.
- **description**
  User defined description.
- **glob**
  Displays the items that match the **glob** expression. See **help glob** for a description of **glob** expression syntax.
- **name**
  Specifies a unique name for the component. This option is required for the commands **create**, **delete**, and **modify**.
- **partition**
  Displays the administrative partition within which the component resides.
- **regex**
  Displays the items that match the regular expression. The regular expression must be preceded by an at sign (@[regular expression]) to indicate that the identifier is a regular expression. See **help regex** for a description of regular expression syntax.
- **source**
  Specifies the string that you want to rewrite. The default value is **none**.
- **target**
  Specifies the new string, to replace the **source** string. The default value is **none**.

- **to-folder**
  stream profiles can be moved to any folder under **/Common**, but configuration dependencies may restrict moving the profile out of **/Common**.

See Also

create, *delete*, *edit*, glob, *list*, *virtual*, *modify*, *mv*, regex, *reset-stats*, *show*, *tmsh*

tcp

Configures a Transmission Control Protocol (TCP) profile.

Syntax

Configure the **tcp** component within the **ltm profile** module using the syntax shown in the following sections.

Create/Modify

```
create tcp [name]
modify tcp [name]
    abc [disabled | enabled]
    ack-on-push [disabled | enabled]
    app-service [[string] | none]
    close-wait-timeout [integer]
    cmetrics-cache [disabled | enabled]
    congestion-control [high-speed | new-reno | none | reno | scalable |
        vegas | illinois | woodside | chd | cdg | cubic | westwood]
    defaults-from [ [name] | none]
    deferred-accept [disabled | enabled]
    delay-window-control [disabled | enabled]
    delayed-acks [disabled | enabled]
    delay-window-control [disabled | enabled]
    description [string]
    dsack [disabled | enabled]
    early-retransmit [disabled | enabled]
    ecn [disabled | enabled]
    fin-wait-timeout [integer]
    hardware-syn-cookie [disabled | enabled]
    idle-timeout [integer]
    init-cwnd [integer]
    init-rwnd [integer]
    ip-tos-to-client [integer]
    keep-alive-interval [integer]
    limited-transmit [disabled | enabled]
    link-qos-to-client [integer]
    max-retrans [integer]
    md5-signature [disabled | enabled]
    md5-signature-passphrase [none | [string] ]
    minimum-rto [integer]
    mptcp [disabled | enabled]
    mptcp-csum [disabled | enabled]
    mptcp-csum-verify [disabled | enabled]
    mptcp-debug [disabled | enabled]
    mptcp-fallback [reset | retransmit | activeaccept | accept]
    mptcp-joinmax [integer]
    mptcp-nojoindssack [disabled | enabled]
    mptcp-rtomax [integer]
    mptcp-rxmitmin [integer]
    mptcp-subflowmax [integer]
    mptcp-makeafterbreak [disabled | enabled]
    mptcp-timeout [integer]
    mptcp-fastjpoin [disabled | enabled]
    nagle [disabled | enabled]
    pkt-loss-ignore-rate [integer]
```

```
    pkt-loss-ignore-burst [integer]
    proxy-buffer-high [integer]
    proxy-buffer-low [integer]
    proxy-mss [disabled | enabled]
    proxy-options [disabled | enabled]
    rate-pace [disabled | enabled]
    receive-window-size [integer]
    reset-on-timeout [disabled | enabled]
    selective-acks [disabled | enabled]
    selective-nack [disabled | enabled]
    send-buffer-size [integer]
    slow-start [disabled | enabled]
    syn-cookie-whitelist [disabled | enabled]
    syn-max-retrans [integer]
    syn-rto-base [integer]
    tail-loss-probe [disabled | enabled]
    time-wait-recycle [disabled | enabled]
    time-wait-timeout [integer]
    timestamps [disabled | enabled]
    verified-accept [disabled | enabled]
    zero-window-timeout [integer]
edit tcp [ [ [name] | [glob] | [regex] ] ... ]
    all-properties
    non-default-properties
reset-stats tcp
reset-stats tcp [ [ [name] | [glob] | [regex] ] ... ]
```

Display

```
list tcp
list tcp  [ [ [name] | [glob] | [regex] ] ... ]
show running-config tcp
show running-config tcp
  [ [ [name] | [glob] | [regex] ] ... ]
    all-properties
    non-default-properties
    one-line
    partition
show tcp
show tcp [ [ [name] | [glob] | [regex] ] ... ]
    (default | exa | gig | kil | meg | peta | raw | tera | yotta | zetta)
    field-fmt
    global
```

Delete

```
delete tcp [name]
```

Description

You can use the **tcp** component to manage TCP network traffic. Many of the options are standard SYSCTL-types of options, while others are unique to the traffic management system. For most of the options, the default values usually meet your needs. The specific options that you might want to change are: **reset-on-timeout**, **idle-timeout**, **ip-tos-to-client**, and **link-qos-to-client**.

The system installation includes these default TCP-type profiles: **tc**, **tcp-cell-optimized**, **tcp-lan-optimized**, and **tcp-wan-optimized**. You can modify the settings of these profiles, or create new TCP-type profiles using any of these existing profiles as parent profiles.

Examples

create tcp my_tcp_profile defaults-from tcp

Creates a custom TCP profile named **my_tcp_profile** that inherits its settings from the system default tcp profile.

list tcp all-properties

Displays all properties for all TCP profiles

Options

- **abc**
  When **enabled**, increases the congestion window by basing the increase amount on the number of previously unacknowledged bytes that each acknowledgement code (ACK) includes. The default value is **enabled**.
- **ack-on-push**
  When enabled, significantly improves performance to Microsoft® Windows® and MacOS peers, who are writing out on a very small send buffer. The default value is **enabled**.
- **app-service**
  Specifies the name of the application service to which the profile belongs. The default value is **none**. **Note:** If the **strict-updates** option is **enabled** on the application service that owns the object, you cannot modify or delete the profile. Only the application service can modify or delete the profile.
- **close-wait-timeout**
  Specifies the number of seconds that a connection remains in a LAST-ACK (last acknowledgement code) state before quitting. A value of **0** (zero) represents a term of forever (or until the matrix of the FIN state). The default value is **5** seconds.
- **cmetrics-cache**
  Specifies, when **enabled**, the default value, that the system uses a cache for storing congestion metrics.
- **congestion-control**
  Specifies the algorithm to use to share network resources among competing users to reduce congestion. The default value is **high-speed**. The options are:
  - **cdg**
    Specifies that the system use a Caia Delay-Gradient congestion control algorithm, where congestion inferences are made based on a gradient of RTT over time. Improves inferences made about packet

loss and whether they are due to congestion or other factors. The use of a shadow window improves coexistence with loss-based TCP flows.

- **chd**
  Specifies that the system use a Caia-Hamilton delay-based congestion control algorithm, where delay-based congestion window operations are performed only once per RTT. Tolerates packet losses that are likely to be unrelated to congestion. Uses a shadow window to help regain lost transmission opportunities when competing with loss-based TCP flows.
- **cubic**
  Specifies that the system uses a component optimized for high latency, high bandwidth connections as the TCP congestion control algorithm.
- **high-speed**
  Specifies that the system uses a more aggressive, loss-based algorithm.
- **illinois**
  Specifies that the system uses a hybrid of both delay and loss as the TCP congestion control algorithm.
- **new-reno**
  Specifies that the system uses a modification to the Reno algorithm that responds to partial acknowledgements when SACKs are unavailable.
- **none**
  Specifies that the system does not use a network-congestion-control mechanism, even when congestion occurs.
- **reno**
  Specifies that the system uses an implementation of the TCP Fast Recovery algorithm, which is based on the implementation in the BSD Reno release.
- **scalable**
  Specifies that the system uses a TCP algorithm modification that adds a scalable, delay-based and loss-based component into the Reno algorithm.
- **vegas**
  Specifies that the system uses a delay-based component as the TCP congestion control algorithm.
- **westwood**
  Specifies that the system uses the Westwood+ bandwidth estimation component as the TCP congestion control algorithm.
- **woodside**
  Specifies that the system uses a hybrid of both delay and loss as the TCP congestion control algorithm.

- **defaults-from**
  Specifies the profile that you want to use as the parent profile. Your new profile inherits all settings and values from the parent profile. The default value is **tcp**.
- **deferred-accept**
  Specifies, when **enabled**, that the system defers allocation of the connection chain context until the system has received the payload from the client. This option is useful for dealing with 3-way handshake denial-of-service (DOS) attacks. The default value is **disabled**.
- **delay-window-control**
  When **enabled**, the system uses an estimate of queueing delay as a measure of congestion, in addition to the normal loss-based control, to control the amount of data sent. The default value is **disabled**.
- **delayed-acks**
  Specifies, when **enabled**, the default value, that the traffic management system allows coalescing of multiple acknowledgement (ACK) responses.
- **description**
  User defined description.
- **dsack**
  When **enabled**, specifies the use of the SACK option to acknowledge duplicate segments. The default is **disabled**.
- **early-retransmit**
  Specifies, when **enabled**, that the system uses early retransmit recovery (as specified in RFC 5827) to reduce the recovery time for connections that are receive-buffer or user-data limited. The default value is **disabled**.
- **ecn**
  Specifies, when **enabled**, that the system uses the TCP flags CWR and ECE to notify its peer of congestion and congestion counter-measures. The default value is **disabled**.
- **fin-wait-timeout**
  Specifies the number of seconds that a connection is in the FIN-WAIT or closing state before quitting. The default value is **5** seconds. A value of **0** (zero) represents a term of forever (or until the matrix of the FIN state).
- **glob**
  Displays the items that match the **glob** expression. See **help glob** for a description of **glob** expression syntax.
- **hardware-syn-cookie**
  Specifies whether or not to use hardware SYN Cookie when cross system limit. The default value is **disabled**.
- **idle-timeout**
  Specifies the number of seconds that a connection is idle before the connection is eligible for deletion. The default value is **300** seconds.
- **init-cwnd**
  Specifies the initial congestion window size for connections to this destination. The actual window size is this value multiplied by the MSS

(Maximal Segment Size) for the same connection. The default value is **0** (zero), which means to use the values specified in RFC2414. The range is from **0** to **16**.

- **init-rwnd**
  Specifies the initial receive window size for connections to this destination. The actual window size is this value multiplied by the MSS (Maximal Segment Size) for the same connection. The default value is **0** (zero), which means to use the Slow Start value. The range is from **0** to **16**.
- **ip-tos-to-client**
  Specifies the Type of Service (ToS) level that the traffic management system assigns to TCP packets when sending them to clients. The default value is **0** (zero).
- **keep-alive-interval**
  Specifies the keep-alive probe interval, in seconds. The default value is **1800** seconds.
- **limited-transmit**
  Specifies, when **enabled**, the default value, that the system uses limited transmit recovery revisions for fast retransmits (as specified in RFC 3042) to reduce the recovery time for connections on a lossy network.
- **link-qos-to-client**
  Specifies the Link Quality of Service (QoS) level that the system assigns to TCP packets when sending them to clients. The default value is **0** (zero).
- **max-retrans**
  Specifies the maximum number of retransmissions of data segments that the system allows. The default value is **8**.
- **md5-signature**
  Specifies, when **enabled**, that the system uses RFC2385 TCP-MD5 signatures to protect TCP traffic against intermediate tampering. The default value is **disabled**.
- **md5-signature-passphrase**
  Specifies a plain text passphrase which may be between **1** and **80** characters in length, and is used in a shared-secret scheme to implement the spoof-prevention parts of RFC2385. The default value is **none**.
- **minimum-rto**
  Specifies the minimum TCP retransmission timeout in milliseconds. The default value is **0** milliseconds; which means using the TCP stack default.
- **mptcp**
  Specifies, when **enabled**, that the system will accept MPTCP connections. The default value is **disabled**.
- **mptcp-csum**
  Specifies, when **enabled**, that the system will calculate the checksum for MPTCP connections. The default value is **disabled**.

- **mptcp-csum-verify**
  Specifies, when **enabled**, that the system verifys checksum for MPTCP connections. The default value is **disabled**.
- **mptcp-debug**
  Specifies, when **enabled**, that the system provides debug logs and statistics for MPTCP connections. The default value is **disabled**.
- **mptcp-fallback**
  Specifies, MPTCP fallback mode. The default value is **reset**.
  The options are:
  - **accept**
    Specifies accept on fallback.
  - **active-accept**
    Specifies active accept on fallback.
  - **reset**
    Specifies that the connection is reset on fallback.
  - **retransmit**
    Specifies retransmit on fallback.
- **mptcp-joinmax**
  Specifies the max number of MPTCP connections that can join to given one. The default value is **5**.
- **mptcp-nojoindssack**
  Specifies, when **enabled**, no DSS option is sent on the JOIN ACK. The default value is **disabled**.
- **mptcp-rtomax**
  Specifies, the number of RTOs before declaring subflow dead. The default value is **5**.
- **mptcp-rxmitmin**
  Specifies the minimum value (in msec) of the retransmission timer for these MPTCP flows. The default value is **1000**.
- **mptcp-subflowmax**
  Specifies the maximum number of MPTCP subflows for a single flow. The default value is **6**.
- **mptcp-makeafterbreak**
  Specifies, when **enabled**, that make-after-break functionality is supported, allowing for long-lived MPTCP sessions. The default value is **disabled**.
- **mptcp-timeout**
  Specifies, the timeout value to discard long-lived sessions that do not have an active flow, in seconds. The default value is **3600**.
- **mptcp-fastjoin**
  Specifies, when **enabled**, FAST join, allowing data to be sent on the MP_JOIN SYN, which can allow a server response to occur in parallel with the JOIN. The default value is **disabled**.
- **nagle**
  Specifies, when **enabled**, that the system applies Nagle's algorithm to reduce the number of short segments on the network. The default value is

disabled.
Note that for interactive protocols such as Telnet, rlogin, or SSH, F5 Networks recommends disabling this setting on high-latency networks, to improve application responsiveness.

- **name**
  Specifies a unique name for the component. This option is required for the commands **create**, **delete**, and **modify**.
- **partition**
  Displays the administrative partition within which the profile resides.
- **pkt-loss-ignore-burst**
  Specifies the probability of performing congestion control when multiple packets in a row are lost, even if the **pkt-loss-ignore-rate** was not exceeded. Valid values are **0** (zero) through **32**. The default value is **0** (zero), which means that the system performs congestion control, if any packets are lost. Higher values decrease the chance of performing congestion control.
- **pkt-loss-ignore-rate**
  Specifies the threshold of packets lost per million at which the system should perform congestion control. Valid values are **0** (zero) through **1,000,000**. The default value is **0** (zero), which means that the system performs congestion control, if any packet loss occurs. If you set the ignore rate to **10** and packet loss for a TCP connection is greater than 10 per million, congestion control occurs.
- **proxy-buffer-high**
  Specifies the highest level at which the receive window is closed. The default value is **49152**.
- **proxy-buffer-low**
  Specifies the lowest level at which the receive window is closed. The default value is **32768**.
- **proxy-mss**
  Specifies, when enabled, that the system advertises the same mss to the server as was negotiated with the client. The default value is **disabled**.
- **proxy-options**
  Specifies, when **enabled**, that the system advertises an option, such as a time-stamp to the server only if it was negotiated with the client. The default value is **disabled**.
- **rate-pace**
  Specifies, when **enabled**, that the system will rate pace TCP data transmissions. The default value is **disabled**.
- **receive-window-size**
  Specifies the size of the receive window, in bytes. The default value is **65535** bytes.
- **regex**
  Displays the items that match the regular expression. The regular expression must be preceded by an at sign (@[regular expression]) to indicate that the identifier is a regular expression. See **help regex** for a description of regular expression syntax.

- **reset-on-timeout**
  Specifies whether to reset connections on timeout. The default value is **enabled**.
- **selective-acks**
  Specifies, when **enabled**, the default value, that the system negotiates RFC2018-compliant Selective Acknowledgements with peers.
- **selective-nack**
  Specifies whether Selective Negative Acknowledgment is **enabled** or **disabled**. The default value is **enabled**.
- **send-buffer-size**
  Specifies the size of the buffer, in bytes. The default value is **65535** bytes.
- **slow-start**
  Specifies, when **enabled**, the default value, that the system uses larger initial window sizes (as specified in RFC 3390) to help reduce round trip times. Note that disabling this attribute causes the setting for **cmetrics-cache** to be ignored.
- **syn-cookie-whitelist**
  Specifies whether or not to use a SYN Cookie WhiteList when doing software SYN Cookies. This means not doing a SYN Cookie for the same src IP address if it has been done already in the previous tm.flowstate.timeout (30) seconds. The default value is **disabled**.
- **syn-max-retrans**
  Specifies the maximum number of retransmissions of SYN segments that the system allows. The default value is **3**.
- **syn-rto-base**
  Specifies the initial RTO (Retransmission TimeOut) base multiplier for SYN retransmission, in milliseconds. This value is modified by the exponential backoff table to select the interval for subsequent retransmissions. The default value is **0**.
- **tail-loss-probe**
  Specifies whether the system uses tail loss probe to reduce the number of retransmission timeouts. The default value is **disabled**.
- **time-wait-recycle**
  Specifies whether the system recycles the connection when a SYN packet is received in a TIME-WAIT state. The default value is **enabled**.
- **time-wait-timeout**
  Specifies the number of milliseconds that a connection is in the TIME-WAIT state before closing. The default value is **2000** milliseconds. The range is from **0** to **600,000** (10 minutes).
- **timestamps**
  Specifies, when **enabled**, the default value, that the system uses the timestamps extension for TCP (as specified in RFC 1323) to enhance high-speed network performance.
- **verified-accept**
  Specifies, when **enabled**, that the system can actually communicate with the server before establishing a client connection. To determine this, the

system sends the server a SYN before responding to the client's SYN with a SYN-ACK. When disabled, the system accepts the client connection before selecting a server to talk to. This option is not compatible with iRules. The default value is **disabled**.

- **zero-window-timeout**
  Specifies the timeout in milliseconds for terminating a connection with an effective zero length TCP transmit window. The timeout starts when the peer advertises a zero length TCP window or when enough data has been sent to fill the previously advertised window. The timer is canceled when a non-zero length window is received. The default is **20000** milliseconds.

See Also

create, *delete*, *edit*, glob, *list*, *virtual*, *modify*, regex, *reset-stats*, *show*, *tmsh*

udp

Configures a User Datagram Protocol (UDP) profile.

Syntax

Configure the **udp** component within the **ltm profile** module using the syntax shown in the following sections.

Create/Modify

```
create udp [name]
modify udp [name]
    allow-no-payload [disabled | enabled]
    app-service [[string] | none]
    datagram-load-balancing [disabled | enabled]
    defaults-from [[name] | none]
    description [string]
    idle-timeout [immediate | indefinite | integer]
    ip-tos-to-client [[integer] | pass-through]
    link-qos-to-client [[integer] | pass-through]
    no-checksum [disabled | enabled]
    proxy-mss [disabled | enabled]
edit udp [ [ [name] | [glob] | [regex] ] ... ]
    all-properties
    non-default-properties
mv udp [ [[source-name] [destination-name]] | [[name] to-folder [folder-name]] |
[[name...name] to-folder [folder-name]] ]
    to-folder
reset-stats udp
reset-stats udp [ [ [name] | [glob] | [regex] ] ... ]
```

Display

```
list udp
list udp [ [ [name] | [glob] | [regex] ] ... ]
show running-config udp
show running-config udp
  [ [ [name] | [glob] | [regex] ] ... ]
    all-properties
    non-default-properties
    one-line
    partition
show udp
show udp [ [ [name] | [glob] | [regex] ] ... ]
    (default | exa | gig | kil | meg | peta | raw | tera | yotta | zetta)
    field-fmt
    global
```

Delete

```
delete udp [name]
```

Description

You can use the **udp** component to manage UDP network traffic.

Examples

create udp my_udp_profile defaults-from udp

Creates a custom UDP profile named **my_udp_profile** that inherits its settings from the system default UDP profile.

list udp all-properties

Displays all properties for all UDP profiles.

mv udp /Common/my_udp_profile to-folder /Common/my_folder

Moves a custom udp profile named **my_udp_profile** to a folder named **my_folder**, where **my_folder** has already been created and exists within **/Common**.

Options

- **allow-no-payload**
  Provides the ability to allow the passage of datagrams that contain header information, but no essential data. The default is **disabled**.
- **app-service**
  Specifies the name of the application service to which the profile belongs. The default value is **none**. **Note:** If the **strict-updates** option is **enabled** on the application service that owns the object, you cannot modify or delete the profile. Only the application service can modify or delete the profile.
- **datagram-load-balancing**
  Provides the ability to load balance UDP datagram by datagram. The default is **disabled**.
- **defaults-from**
  Specifies the profile that you want to use as the parent profile. Your new profile inherits all settings and values from the parent profile. The default value is **udp**.
- **description**
  User defined description.
- **glob**
  Displays the items that match the **glob** expression. See **help glob** for a description of **glob** expression syntax.
- **idle-timeout**
  Specifies the number of seconds that a connection is idle before the connection is eligible for deletion. The default value is **60** seconds.

- **ip-tos-to-client**
  Specifies the Type of Service level that the traffic management system assigns to UDP packets when sending them to clients. The default value is **0** (zero).
- **link-qos-to-client**
  Specifies the Quality of Service level that the system assigns to UDP packets when sending them to clients. The default value is **0** (zero).
- **name**
  Specifies a unique name for the component. This option is required for the commands **create**, **delete**, and **modify**.
- **no-checksum**
  Enables or disables checksum processing. Note that if the datagram is IPv6, the system always performs checksum processing. The default value is **disabled**.
- **partition**
  Displays the administrative partition within which the profile resides.
- **proxy-mss**
  Specifies, when enabled, that the system advertises the same mss to the server as was negotiated with the client. The default value is **disabled**.
- **regex**
  Displays the items that match the regular expression. The regular expression must be preceded by an at sign (@[regular expression]) to indicate that the identifier is a regular expression. See **help regex** for a description of regular expression syntax.
- **to-folder**
  udp profiles can be moved to any folder under **/Common**, but configuration dependencies may restrict moving the profile out of **/Common**.

See Also

create, *delete*, *edit*, glob, *ltm profile*, *virtual*, *modify*, *mv*, *show*, regex, *reset-stats*, *tmsh*

wa-cache

Manages the BIG-IP® system WebAccelerator cache.

Syntax

Configure the **wa-cache** component within the **ltm profile** module using the syntax shown in the following sections.

Delete

```
delete wa-cache [name]
```

Description

You can use the **wa-cache** component to delete the entries in the BIG-IP® system WebAccelerator cache.

Examples

delete wa-cache

Deletes the entries in the BIG-IP system WebAccelerator cache.

See Also

delete, *tmsh*

web-acceleration

Configures a Web Acceleration profile.

Syntax

Configure the **web-acceleration** component within the **ltm profile** module using the syntax shown in the following sections.

Create/Modify

```
create web-acceleration [name]
modify web-acceleration [name]
    applications
      [add | delete | modify | replace-all-with] {
        [application] ...
    }
    applications none
    app-service [[string] | none]
    cache-aging-rate [integer]
    cache-client-cache-control-mode [all | max-age | none]
    cache-insert-age-header [disabled | enabled]
    cache-max-age [integer]
    cache-max-entries [integer]
    cache-object-max-size [integer]
    cache-object-min-size [integer]
    cache-size [integer]
    cache-uri-exclude
      [add | delete | replace-all-with] {
        [URI] ...
    }
    cache-uri-exclude none
    cache-uri-include
      [add | delete | replace-all-with]{
        [URI] ...
    }
    cache-uri-include .*
    cache-uri-include-override
      [add | delete | replace-all-with]{
        [URI] ...
    }
    cache-uri-include-override none
    cache-uri-pinned
      [add | delete | replace-all-with] {
        [URI] ...
    }
    cache-uri-pinned none
    metadata-cache-max-size 25
    defaults-from [ [name] | none]
    description [string]
edit web-acceleration [ [ [name] | [glob] | [regex] ] ... ]
    all-properties
    non-default-properties
reset-stats web-acceleration
reset-stats web-acceleration [ [ [name] | [glob] | [regex] ] ... ]
```

Display

```
list web-acceleration
list web-acceleration [ [ [name] | [glob] | [regex] ] ... ]
show running-config web-acceleration
show running-config web-acceleration [ [ [name] | [glob] | [regex] ]
                                       ... ]
    all-properties
    non-default-properties
    one-line
    partition
show web-acceleration
show web-acceleration [ [ [name] | [glob] | [regex] ] ... ]
     (default | exa | gig | kil | meg | peta | raw | tera | yotta | zetta)
     field-fmt
     global
```

Delete

```
delete web-acceleration [name]
```

Description

You can use the **web-acceleration** component to create, modify, display, or delete an Web Acceleration profile.

The BIG-IP® system installation includes the following default Web Acceleration-type profiles:

- **web-acceleration**
- **optimized-caching**
- **optimized-acceleration**

The default Web Acceleration profile contains values for properties related to managing WA Cache.

You can create a new Web Acceleration-type profile using an existing profile as a parent profile, and then you can change the values of the properties to suit your needs.

Examples

create web-acceleration my_wa_profile defaults-from web-acceleration

Creates a custom Web Acceleration profile named **my_wa_profile** that inherits its settings from the system default Web Acceleration profile.

Options

- **applications**
  Configures a list of applications assigned to this profile. Assigning at least one application enables WA functionality. The default value of **none** specifies that WA is not enabled.
- **app-service**
  Specifies the name of the application service to which the profile belongs. The default value is **none**. **Note:** If the **strict-updates** option is **enabled** on the application service that owns the object, you cannot modify or delete the profile. Only the application service can modify or delete the profile.
- **cache-aging-rate**
  Specifies how quickly the system ages a cache entry. The aging rate ranges from **0** (slowest aging) to **10** (fastest aging). The default value is **9**.
- **cache-client-cache-control-mode**
  Specifies which cache disabling headers sent by clients the system ignores. The default value is **all**.
- **cache-insert-age-header**
  When **enabled**, inserts Age and Date headers in the response. The default value is **enabled**.
- **cache-max-age**
  Specifies how long the system considers the cached content to be valid. The default value is **3600** seconds.
- **cache-max-entries**
  Specifies the maximum number of entries that can be in the WA cache. The default value is **10000**.
- **cache-object-max-size**
  Specifies the largest object that the system considers eligible for caching. The default value is **50000** bytes.
- **cache-object-min-size**
  Specifies the smallest object that the system considers eligible for caching. The default value is **500** bytes.
- **cache-size**
  Specifies the maximum size, in megabytes, for the WA cache. When the cache reaches the maximum size, the system starts removing the oldest entries. The default value is **100** megabytes.
- **cache-uri-exclude**
  Configures a list of Uniform Resource Identifiers (URIs) to exclude from the WA Cache. The default value is **none** and specifies that no URI will be excluded.
- **cache-uri-include**
  Configures a list of URIs that are cacheable. The default value is **.*** and specifies that all URIs are cacheable.
- **cache-uri-include-override**
  Configures a list of URIs that should be cached in the WA cache even though they would normally not be cached due to constraints defined by

cache-object-max-size or others. The default value is **none**. URIs on the **cache-uri-include-override** list are cacheable even if they are not on the **cache-uri-include** list.

- **cache-uri-pinned**
  Configures a list of URIs that are kept in the WA cache regardless their max-age or expiry settings. The default value is **none**. URIs on the **cache-uri-pinned** list are cacheable even if they are not on the **cache-uri-include** list.
- **metadata-cache-max-size**
  Specifies the maximum size of the metadata cache. The metadata cache applies only when there is an application applied to the profile, and does not include the content cache.
- **defaults-from**
  Configures the profile that you want to use as the parent profile. Your new profile inherits all settings and values from the parent profile specified. The default value is **webacceleration**.
- **description**
  User defined description.
- **partition**
  Displays the administrative partition within which the profile resides.

See Also

create, *delete*, *edit*, glob, *list*, *fasthttp*, *virtual*, *modify*, regex, *reset-stats*, *show*, *tmsh*

web-security

Configures a Web Security profile.

Syntax

Configure the **web-security** component within the **ltm profile** module using the syntax shown in the following sections.

Create/Modify

```
create web-security [name]
modify web-security [name]
    defaults-from [ [name] | none]
edit web-security [ [ [name] | [glob] | [regex] ] ... ]
    all-properties
    non-default-properties
```

Display

```
list web-security
list web-security [ [ [name] | [glob] | [regex] ] ... ]
                                          ... ]
    all-properties
    non-default-properties
    one-line
    partition
```

Delete

```
delete web-security [name]
```

Description

You can use the **web-security** component to create, modify, display, or delete an Web Security profile.

The BIG-IP® system installation includes the following default Web Security-type profiles:

- **websecurity**

The default Web Security profile contains values for properties related to managing web security.

You can create a new Web Security-type profile using an existing profile as a parent profile, and then you can change the values of the properties to suit your needs.

Examples

create web-security my_asm_profile defaults-from web-security

Creates a custom Web Security profile named **my_asm_profile** that inherits its settings from the system default Web Security profile.

Options

- **defaults-from**
  Configures the profile that you want to use as the parent profile. Your new profile inherits all settings and values from the parent profile specified. The default value is **none**.
- **partition**
  Displays the administrative partition within which the profile resides.

See Also

create, *delete*, *edit*, glob, *list*, *fasthttp*, *virtual*, *modify*, regex, *reset-stats*, *show*, *tmsh*

xml

Configures an XML profile.

Syntax

Configure the **xml** component within the **ltm profile** module using the syntax shown in the following sections.

Create/Modify

```
create xml [name]
modify xml [name]
    app-service [[string] | none]
    defaults-from [ [name] | none]
    description [string]
    namespace-mappings [ [none] |
          [ { { mapping-namespace namespace1 mapping-prefix prefix1 } } ]
    xpath-queries [ none |
          [ add | delete | replace_all_with { queries } ] ]
    multiple-query-matches [enabled | disabled]
edit xml [ [ [name] | [glob] | [regex] ] ... ]
    all-properties
    non-default-properties
mv xml [ [[source-name] [destination-name]] | [[name] to-folder [folder-name]] |
[[name...name] to-folder [folder-name]] ]
    to-folder
```

Display

```
list xml
list xml [ [ [name] | [glob] | [regex] ] ... ]
show running-config xml
show running-config xml [ [ [name] | [glob] | [regex] ] ... ]
    all-properties
    non-default-properties
    one-line
    partition
```

Delete

```
delete xml [name]
```

Description

Use this command to create, modify, display, or delete an XML profile with which you can use XML functionality.

Examples

create xml my_xml_profile defaults-from xml

Creates a custom XML profile named **my_xml_profile** that inherits its settings from the system default XML profile.

list xml

Displays the properties of all XML profiles.

mv xml /Common/my_xml_profile to-folder /Common/my_folder

Moves a custom xml profile named **my_xml_profile** to a folder named **my_folder**, where **my_folder** has already been created and exists within **/Common**.

Options

- **app-service**
  Specifies the name of the application service to which the profile belongs. The default value is **none**. **Note:** If the **strict-updates** option is **enabled** on the application service that owns the object, you cannot modify or delete the profile. Only the application service can modify or delete the profile.
- **defaults-from**
  Specifies the profile that you want to use as the parent profile. Your new profile inherits all settings and values from the parent profile specified. The default value is **xml**.
- **description**
  User defined description.
- **glob**
  Displays the items that match the **glob** expression. See **help glob** for a description of **glob** expression syntax.
- **name**
  Specifies a unique name for the component. This option is required for the commands **create**, **delete**, and **modify**.
- **partition**
  Displays the administrative partition within which the component resides.
- **namespace-mappings**
  Specifies a list of mappings between namespaces and prefixes to be used in the XPath queries of the profile.
- **regex**
  Displays the items that match the regular expression. The regular expression must be preceded by an at sign (@[regular expression]) to indicate that the identifier is a regular expression. See **help regex** for a description of regular expression syntax.

- **to-folder**
  xml profiles can be moved to any folder under **/Common**, but configuration dependencies may restrict moving the profile out of **/Common**.
- **xpath-queries**
  Specifies the list of XPath queries that are used by the profile. A match of any of the queries will trigger the XML_CONTENT_BASED_ROUTING iRule event.
- **multiple-query-matches**
  Enables or disables multiple matches for a single XPath query.

See Also

create, *delete*, *edit*, glob, *list*, *virtual*, *modify*, *mv*, regex, *reset-stats*, *show*, *tmsh*

68

net

- Introducing the net module
- Alphabetical list of components

Introducing the net module

You can use the tmsh components that reside within the net module to configure the network. For more information about the tmsh hierarchical structure, see Chapter 2, *Understanding and Using the Traffic Management Shell*.

Alphabetical list of components

The remainder of this chapter lists the tmsh components that are available in the net module.

arp

Manages entries in the Address Resolution Protocol (ARP) table.

Syntax

Configure the **arp** component within the **net** module using the syntax in the following sections.

Create/Modify

```
create arp [name]
    description [string]
    ip-address [ip address ... ip address]
    mac-address [mac address]

modify arp [name]
    description [string]
    mac-address [mac address]

edit arp [ [ [name] | [glob] | [regex] ] ... ]
    all-properties
    non-default-properties
=head2 DISPLAY

list arp
list arp [ [ [name] | [glob] | [regex] ] ... ]
show running-config arp
show running-config arp
  [ [ [name] | [glob] | [regex] ] ... ]
    all-properties
    non-default-properties
    one-line

show arp
show arp [ [ [name] | [glob] | [regex] ] ... ]
    (dynamic | static)
```

Delete

```
delete arp [name]
```

Description

You can use the **arp** component to add entries to or delete entries from the ARP table.

You can create static ARP entries for IPv4 addresses to link-layer addresses, such as Ethernet media access control (MAC) addresses. You can view and delete static and dynamic ARP entries.

Note that you can use the **db** component in the **sys** module to configure how the system handles ARP entries for dynamic timeout, maximum dynamic entries, add reciprocal, and maximum retries. For more information, see **sys db**.

Examples

create arp myARP ip-address 10.10.10.20 mac-address 00:0b:09:88:00:9a

Creates an arp mapping of the IP address 10.10.10.20 to the MAC address 00:0b:09:88:00:9a, and the name of this entry is myARP. Alternatively, the address can be used as the name, like the following example.

create arp 10.10.10.20 mac-address 00:0b:09::88:00:9a

Creates an arp mapping of IP address 10.10.10.20 to the MAC address 00:0b:09:88:00:9a.

modify arp 10.10.10.20 mac-address 00:0b:09:88:00:9b

Modifies the ARP mapping of the ARP entry named 10.10.10.20 to the MAC address 00:0b:09:88:00:9b.

show arp

Displays ARP status and statistics for the system.

show arp any%2

Displays ARP status and statistics for all IP addresses in route domain 2. A **glob** expression displays the same result: **show arp *%2**.

list arp all-properties

Displays all properties for all ARP entries for the system.

list arp non-default-properties

Displays all non-default properties for all ARP entries for the system.

delete arp all

Deletes all ARP entries for the system.

delete arp myARP

Deletes the ARP entry named myARP.

Options

- **description**
  User defined description.
- **dynamic**
  Displays the status of dynamic ARP entries.
- **glob**
  Displays the items that match the **glob** expression. See **help glob** for a description of **glob** expression syntax.
- **ip address**
  Specifies the IP address, in one of the following formats, for which you want to configure an ARP entry:
  - IPv4 address in dotted-quad notation, for example, **10.10.10.1**
  - host name, for example, **www.f5.com**

You can also specify a list of IP addresses separated by a single space. For example, this list contains three IP addresses: 10.10.10.20 10.10.10.21 10.10.10.22.

- **ip-address**
  The IP address to be mapped. This is optional, and if not present, the name needs to be a string that represents a valid IP address.
- **mac-address**
  Specifies a 6-byte ethernet address in not case-sensitive hexadecimal colon notation, for example, **00:0b:09:88:00:9a**. You must specify a MAC address when you create an ARP entry.
- **regex**
  Displays the items that match the regular expression. The regular expression must be preceded by an at sign (@[regular expression]) to indicate that the identifier is a regular expression. See **help regex** for a description of regular expression syntax.
- **static**
  Displays the status of static ARP entries.

See Also

create, *delete*, *edit*, glob, *list*, *modify*, regex, *show*, *tmsh*

bwc-policy

Configures a bandwidth control policy for traffic flow.

Syntax

Configure the **bwc-policy** component within the **net** module using the syntax in the following sections.

Create/Modify

```
create bwc-policy [name]
modify bwc-policy [name]
    app-service [[string] | none]
    description [string]
    dynamic [ enabled ]
    max-rate [integer]
    max-user-rate [integer]
    ip-tos [ integer | pass-through]
    link-qos [integer | pass-through]
    measure [ disabled ]
    log-publisher [[string] | none]
    log-period [integer]
    categories [none] {
       max-cat-rate [integer]
       ip-tos [ integer | pass-through]
       link-qos [integer | pass-through]
    }
edit bwc-policy [ [ [name] | [glob] | [regex] ] ... ]
    all-properties
    non-default-properties
```

Display

```
list bwc-policy
list bwc-policy [ [ [name] | [glob] | [regex] ] ... ]
show running-config net bwc-policy
show running-config net bwc-policy [ [ [name] | [glob] | [regex] ] ... ]
    all-properties
    non-default-properties
    one-line
```

Delete

```
delete net bwc-policy [all | [name] ]
```

Description

You can use the **net bwc-policy** to create a bandwidth control policy to handle traffic flow, and then associate it with other components such as packet filter, iRule and virtual server. For details on packet filter, virtual server, please refer to the respective documentation.

Examples

create net bwc-policy

Creates a bwc policy (see below).

list net bwc-policy all-properties

Displays all of the properties of all of the bwc policies.

delete net bwc-policy

Deletes a policy (see below).

Example For Static Policy:

```
net bwc-policy silver_static_policy {
      max-rate 120mbps
}
```

Example For Dynamic Policy:

```
net bwc-policy gold-dynamic-policy {
   categories {
      web {
         description "This is a web test category."
         max-cat-rate 600kbps
         ip-tos 7
         link-qos 5
      }
   }
   description "This is a test."
   dynamic enabled
   max-rate 40gbps
   max-user-rate 1gbps
}
```

Example For Dynamic Policy With Measure Enabled:

```
net bwc-policy gold-dynamic-policy {
   categories {
      web {
         description "This is a web test category."
         max-cat-rate 600kbps
         ip-tos 7
         link-qos 5
      }
   }
   description "This is a test."
   dynamic enabled
   measure enabled
   log_publisher /Common/my_log_publisher
   log-period 2048
   max-rate 40gbps
   max-user-rate 1gbps
}
```

Example For Bwc Using Packet Filter:

```
net bwc-policy bwc {
    max-rate 1mbps
}
```

Define packet filter with bwc on it:

```
net packet-filter pfilter {
    action continue
    bwc-policy bwc
    logging enabled
    order 2
    rule ip
}
```

Example For Bwc Association With Virtual Server:

```
ltm virtual l2-for-virtual {
    destination 0.0.0.0:any
    l2-forward
    mask any
    profiles {
        fastL4 { }
    }
    rules {
        bwc_test
    }
    translate-address disabled
    translate-port disabled
    vlans {
        lan
        wan
    }
    vlans-enabled
}
ltm virtual tcp-passthrough {
    destination 0.0.0.0:http
    ip-protocol tcp
    mask any
    profiles {
        tcp { }
    }
    rules {
        bwc_test
    }
    translate-address disabled
    vlans-disabled
}
```

Example For Delete Bwc Policy:

```
net bwc-policy silver_static_policy
```

Notes: Only static policies are supported for association with packet filter or virtual server components.

Options

- **app-service**
  Specifies the name of the application service to which the object belongs. The default value is **none**. **Note:** If the **strict-updates** option is **enabled** on the application service that owns the object, you cannot modify or delete the object. Only the application service can modify or delete the object.
- **name**
  Specifies a unique name for the policy. This option is required for the commands **create**, **delete**, and **modify**.
- **description**
  User defined description.
- **max-rate**
  Specifies the maximum bandwidth that traffic is allowed using the policy associated. The range is from 1Mbps to 320Gbps.
  Valid units: bps(default), gbps, kbps, mbps.
- **max-user-rate**
  Specifies the maximum bandwidth that traffic is allowed using the policy associated. The range is from 5kbps to 2Gbps.
  Valid units: bps(default), gbps, kbps, mbps.
- **max-cat-rate**
  Specifies the maximum bandwidth that traffic is allowed using this category with associated policy. The range is from 500Kbps to **max-user-rate**.
  Valid units: bps(default), gbps, kbps, mbps.
- **dynamic**
  Specifies the type for policy to be dynamic type. This option is optional for the commands **create**, **delete**, and **modify**. The default valid is disabled. When dynamic is disabled, the policy type is said to be static, where the maximum rate is enforced for combined traffic using the policy and no fairness bandwidth guarantee for each of the traffic respectively. The default value is: disabled. Note: policy type change modification is a disallowed configuration.
  By enabling this option, the policy is dynamic type and requires you to configure **max-user-rate-range**. This type of policy enforces fairness for all the traffic associated with the policy and also for each traffic within the policy.
- **ip-tos**
  Specifies an IP ToS number for the traffic using the **net bwc-policy**. This option specifies the ToS level that the traffic management system assigns

to UDP packets when sending them. The default value is **pass-through**, which indicates, do not modify UDP packets. The valid range for IP ToS value that can be specified is 0 to 63.

◆ Note

If this is specified, bandwidth policy is not enforced. The packets are just marked for a downstream system to process.

- **link-qos**
  Specifies a Link QoS (VLAN priority) for the traffic using the **net bwc-policy**. This option specifies the QoS level that the system assigns to UDP packets when sending. The default value is **pass-through**, which indicates, do not modify UDP packets. The valid range for QoS value is 0 to 7.

◆ Note

If this is specified, bandwidth policy is not enforced. The packets are just marked for a downstream system to process.

- **measure**
  Enables or disables bandwidth measurement on all the future instances of bwc-policy. Users can override this setting using iRules. If enabling measurement on all instances is not desired then users can keep this setting disabled and use iRules to enable measurement on specific instances of bwc policy.
- **log_publisher**
  Specifies the name of the log publisher configured in the system. Bandwidth measurement results will be sent to this log publisher.
- **log_period**
  Time interval in milliseconds representing the frequency of generation of bandwidth measurement logs.
- **categories**
  This specifies the categories under policy. Note: policy need to be enabled as dynamic to configure categories. Up to a maximum of 32 categories can be configured. All the categories under the dynamic policy share the bandwidth as specified for the category, up to a maximum of **max-user-rate**. Specify the maximum bandwidth for the category of traffic using **max-cat-rate** or by **max-cat-rate-percentage** as a percentage of the maximum user rate. Either only the range or absolute value is required.
  Example to configure a dynamic bandwidth policy category using tmsh:

```
root@(localhost)(cfg-sync

Standalone)(Active)(/Common)(tmos.net.bwc-policy.gold-
dynamic-policy)# categories add { web { max-cat-rate
600kbps } }

net bwc-policy gold-dynamic-policy {
  categories {
```

```
        web {
            max-cat-rate 600kbps
        }
    }
    dynamic enabled
    max-rate 40gbps
    max-user-rate 1gbps
}
```

The parameters for dynamic policy and categories:

```
net bwc-policy test-policy {
    app-service none
    categories {
        web {
            app-service none
            description "This is a web test cat"
            max-cat-rate 600kbps
            max-cat-rate-percentage 0
            ip-tos 6
        }
    }
    description "This is a test"
    dynamic enabled
    ip-tos pass-through
    link-qos pass-through
    max-rate 40gbps
    max-user-rate 1gbps
    measure enabled
    log-publisher /Common/my_log_publisher
    log-period 2048
    partition Common
}
```

- **max-cat-rate-percentage**
  Specifies the percentage of the value of the **max-cat-rate** option of the category, which is associated with the **net bwc-policy** component to which this shaping policy is associated, that is available for this traffic flow. The value range is from 500kbps to **max-user-rate**.

iRule

Please refer to iRule documentation for iRule to use bandwidth control policy.

Example To Associate Static Bwc Policy Using iRule:

```
when CLIENT_ACCEPTED {
      BWC::policy attach silver_static_policy
}
```

Example To Associate Dynamic Bwc Policy Using iRule:

```
when CLIENT_ACCEPTED {
      set mycookie [IP::remote_addr]
      BWC::policy attach gold-dynamic-policy $mycookie
}
```

Example For Bwc Policy To Mark Traffic Flows Using iRule:

```
BWC::mark <set|unset> <bwc policy name> <tos <value>> <qos <value>>
```

So to assign a policy, color, and mark here is an example rule

```
when CLIENT_ACCEPTED {
  set mycookie [IP::remote_addr]:[TCP::remote_port]
  BWC::policy attach gold_user $mycookie
  BWC::color set gold_user p2p
  BWC::mark set gold_user tos 8 qos 4
}
```

Example For Using Bwc Policy Category To Color A Flow Using iRule:

After a flow has been assigned a policy, at some later time when the traffic is classified the user can assign an application to this flow. This uses the bwc config to create a bwc policy with the categories keyword: for example, **p2p** category below:

tmsh create net bwc-policy gold_user categories add { p2p { max-cat-rate 8mbps } } max-rate 10mbps max-user-rate 10mbps dynamic enabled

The rule args

```
BWC::color <set|unset> <bwc policy name> <app name>
```

So to assign a policy and color here is an example rule

```
when CLIENT_ACCEPTED {
  set mycookie [IP::remote_addr]:[TCP::remote_port]
  BWC::policy attach gold_user $mycookie
  BWC::color set gold_user p2p
}
```

Example For Bwc Policy Rate Change Using iRule:

After a policy is created, irule can modify the rate for a session or category

The rule args

```
BWC::rate <bwc policy session> <value>
BWC::rate <bwc policy session> <app_name> <value>
```

So to modify the rate

```
when CLIENT_ACCEPTED {
  set mycookie [IP::remote_addr]:[TCP::remote_port]
  BWC::policy attach gold_user $mycookie
  BWC::color set gold_user p2p
  BWC::mark set gold_user tos 8 qos 4
  BWC::rate $mycookie p2p 1000000bps
}
```

Examples For Bwc Policy To Measure The Bandwidth Using iRule:

BWC::measure <<<start|stop> | <identifier id_str> | <get rate|bytes>> <flow|session> [session_str]>

To start the bandwidth measurement for BWC policy

```
when CLIENT_ACCEPTED {
  set mycookie [IP::remote_addr]:[TCP::remote_port]
  BWC::policy attach gold_user $mycookie
  BWC::measure start session
}
```

The above iRule will start the measurement of bandwidth on the gold_user policy instance. The results will be published to the destination specified in the log_publisher setting for the gold_user bwc policy. The measurement results will be logged every 'log_period' amount of time, which is also specified in the policy settings for gold_user.

◆ Note

Attaching a BWC policy is a pre-requisite for all 'BWC::measure.' iRules. Failing to do so will result in the iRule execution failure which in turn will abort the connection.

To start the bandwidth measurement for a flow inside a BWC policy and tag the results.

```
when CLIENT_ACCEPTED {
  set mycookie [IP::remote_addr]:[TCP::remote_port]
  BWC::policy attach gold_user $mycookie
  BWC::measure identifier MYFLOW flow
  BWC::measure start flow
}
```

The above iRule will start the measurement of bandwidth on the current flow or the flow over which the current iRule is running. The results will be published to the destination specified in the log_publisher setting for the gold_user bwc policy. The measurement results will be logged every 'log_period' amount of time, which is also specified in the policy settings for gold_user. Every log message containing the bandwidth result will carry the tag 'MYFLOW'. This helps identify different types of bandwidth results when analyzing the bandwidth measurement results.

To start the bandwidth measurement for a BWC session and get the periodic results.

```
when CLIENT_ACCEPTED {
  set mycookie [IP::remote_addr]:[TCP::remote_port]
  set measureID "MYSESSION"
  BWC::policy attach gold_user $mycookie
  BWC::measure identifier $measureID session
  BWC::measure start session
}
when SERVER_CONNECTED {
  TCP::collect
  set count 0
}
when SERVER_DATA {
    if {$count >= 1000 } {
        set rate [BWC::measure get rate session]
        set bytes [BWC::measure get bytes session]
log local0. "Rate $rate/sec : Bytes $bytes : for address $mycookie"
set count 0
      }
```

```
    TCP::release
    TCP::collect
    incr count
}
```

The above example creates an instance of BWC policy gold_user and enables measurement on it upon the iRule event CLIENT_ACCEPTED. It also starts collecting so that it keeps getting notifed upon the data arrival. For every 1000 packets a measurement of bandwidth is logged. This is an example that illustrates how to measure bandwidth periodically using iRules. Note that the bandwidth measurement results are still sent to configured log_publisher at every log_period interval.

An example log message that is sent to a log publisher.

Apr 2 16:29:04 MYSESSION BWC Measurement: Moving average - 539277 bytes/sec. Total bytes - 7305051

See Also

create, *delete*, *edit*, glob, *list*, *modify*, regex, *show*, *tmsh*

cmetrics

Displays and deletes entries in the route metrics table on the BIG-IP® system.

Syntax

Use the **cmetrics** component within the **net** module to view route metrics or delete a route metric entry using the following syntax.

Display

```
show cmetrics
  option:
    bandwidth
    dest-addr [ip address]
    hwaddress
    mtu
    rtt
    rttvar
    ssthresh
    tmm
```

Delete

```
delete cmetrics
  option:
    dest-addr [IP address]
```

Description

You can use the **cmetrics** component to display entries in the route metrics table on the BIG-IP system. Additionally, you can delete a specified route metric entry from the table. The options are display-only values and cannot be used for filtering.

◆ Note

You can delete only entries that have no connection references.

Examples

show cmetrics

Displays all the entries in the route metrics table.

delete cmetrics dest-addr 10.10.1.11

Deletes the entry with destination IP address 10.10.1.11 from the route metrics table.

Options

- **bandwidth**
  Displays the size of the channel.
- **dest-addr**
  Specifies the destination IP address of the entry that you want to display or delete. You can enter this address in either IPv4 or IPv6 format.
- **hwaddress**
  Displays the Media Access Control (MAC) address for the route.
- **mtu**
  Displays the maximum transmit unit size on the route.
- **rtt**
  Displays the round-trip time on the route.
- **rttvar**
  Displays the variance in the round-trip time.
- **ssthresh**
  Displays the cached slow-start threshold.
- **tmm**
  Displays the identifying number of the tmm (Traffic Management Microkernel).

See Also

delete, *show*, *tmsh*

ike-evt-stat

Displays and resets IKE event statistics

Syntax

Display and reset the **ike-evt-stat** component within the **net** module using the syntax in the following section.

Modify

```
reset-stats ike-evt-stat
```

Display

```
show ike-evt-stat
```

Description

You can use the **ike-evt-stat** component to display and reset IKE event statistics.

Options

For information about the options that you can use with the command **show**, see **help show**.

See Also

reset-stats, *show*, *tmsh*

ike-msg-stat

Displays and resets IKE message statistics

Syntax

Display and reset the **ike-msg-stat** component within the **net** module using the syntax in the following section.

Modify

```
reset-stats ike-msg-stat
```

Display

```
show ike-msg-stat
```

Description

You can use the **ike-msg-stat** component to display and reset IKE message statistics.

Options

For information about the options that you can use with the command **show**, see **help show**.

See Also

reset-stats, *show*, *tmsh*

interface

Configures the parameters of interfaces.

Syntax

Configure the **interface** component within the **net** module using the syntax in the following sections.

Modify

```
modify interface [name]
    description [string]
    [disabled | enabled]
    flow-control (none |rx | tx | tx-rx)
    force-gigabit-fiber [enabled | disabled]
    media [auto | 10baseT half | 10baseT full | 100baseTX half |
          100baseTX full | 1000baseT half | 1000baseT full |
          1000baseSX full | 1000baseLX full | 1000baseCX full |
          10GbaseT full | 10GbaseSR full | 10GbaseLR full |
          10GbaseER full | 10SFP+Cu full | 40GbaseSR4 full |
          40GbaseLR4 full | none | no-phy]
    media-fixed [auto | 10baseT half | 10baseT full |
                100baseTX half | 100baseTX full | 1000baseT half |
                1000baseT full | none | no-phy]
    media-sfp [auto | 10baseT half | 10baseT full | 100baseTX half |
              100baseTX full | 1000baseT half | 1000baseT full |
              1000baseSX full | 1000baseLX full | 1000baseCX full |
              10GbaseT full | 10GbaseSR full | 10GbaseLR full |
              10GbaseER full  | 10SFP+Cu full | 40GbaseSR4 full |
              40GbaseLR4 full | none | no-phy]
    no-mgmt
    prefer-port [fixed | sfp]
    sflow {
        poll-interval [integer]
        poll-interval-global [no | yes]
    }
    stp [disabled | enabled]
    stp-auto-edge-port [enabled | disabled]
    stp-edge-port [false | true]
    stp-link-type [auto | p2p | shared]
    stp-reset
    qinq-ethertype [string]
edit interface [ [ [name] | [glob] | [regex] ] ... ]
    all-properties
    non-default-properties
reset-stats interface
reset-stats interface [ [ [name] | [glob] | [regex] ] ... ]
```

Display

```
list interface
list interface [ [ [name] | [glob] | [regex] ] ... ]
show running-config interface
show running-config interface
  [ [ [name] | [glob] | [regex] ] ... ]
```

```
    all-properties
    mac-address
    media-active
    media-capabilities
    media-max
    mtu
    non-default-properties
    (pending | not-pending)
    one-line
show interface
show interface [ [ [name] | [glob] | [regex] ] ... ]
    all-properties
    (default | exa | gig | kil | meg | peta | raw | tera | yotta | zetta)
    field-fmt
```

Description

You can use the **interface** component to enable or disable an interface, and to display and set media options, duplex mode, and status for an interface. In addition, you can specify whether the interface participates in the spanning tree protocol (STP) configuration, and set per-interface STP parameters such as link type, edge port status, and automatic edge port detection.

Examples

modify interface 1.1 enabled

Enables the interface named **1.1**.

modify interface 1.2 disabled

Disables the interface named **1.2**.

modify interface 1.1 1.2 1.3 stp disable

Disables STP on the interfaces named **1.1**, **1.2**, and **1.3**.

modify interface 1.1 1.2 1.3 stp-auto-edge-port enabled

Sets auto edge detection for STP on the interfaces named **1.1**, **1.2**, and **1.3**.

modify interface 1.1 1.2 1.3 stp-edge-port true

Sets the edge port attribute for STP on the interfaces named **1.1**, **1.2**, and **1.3**.

Options

- **description**
  User defined description.
- **[disabled | enabled]**
  Enables or disables the specified interface. The default value is **enabled**.
- **flow-control**
  Specifies how the system controls the sending of PAUSE frames for flow control. The default value is **tx-rx**.

- **none**
  Disables flow control.
- **rx**
  Specifies that the interface honors pause frames from its partner, but does not generate pause frames.
- **tx**
  Specifies that the interface ignores pause frames from its partner, and generates pause frames when necessary.
- **tx-rx**
  Specifies that the interface honors pause frames from its partner, and also generates pause frames when necessary.

◆ **force-gigabit-fiber**
Enables or disables forcing of gigabit fiber media. If this is enabled for a gigabit fiber interface, the media setting will be forced, and no auto-negotiation will be performed. If it is disabled, auto-negotiation will be performed with just a single gigabit fiber option advertised.

◆ **glob**
Displays the items that match the **glob** expression. See **help glob** for a description of **glob** expression syntax.

◆ **if-index**
Displays the index assigned to this interface. It is a unique identifier assigned for all objects displayed in the SNMP IF-MIB.

◆ **mac-address**
Displays the 6-byte ethernet address in not case-sensitive hexadecimal colon notation, for example, **00:0b:09:88:00:9a**.

◆ **media**
Specifies the settings for the interface. The possible values are: 10baseT-full, 10baseT-half, 10GbaseER full, 10GbaseLR-full, 10GbaseSR-full, 10GbaseT-full, 10SFP+Cu-full, 40GbaseSR4-full, 40GbaseLR4-full, 100baseTX-half, 100baseTX-full, 1000baseLX full, 1000baseCX-full, 1000baseT-full, 1000baseT-half, 1000baseSX-full, auto, none, and no-phy.
When you set the **media** option, the system automatically sets either the **media-sfp** or **media-fixed** option, based on whether the interface supports small factor form pluggable (SFP) interfaces, or for combo ports whether SFP is the preferred port.

◆ **media-active**
Displays the current media setting for the interface.

◆ **media-fixed**
Specifies the settings for a fixed (non-pluggable) interface. Use this option only with a combo port to specify the media type for the fixed interface, when it is not the preferred port.

◆ **media-max**
Displays the maximum media value for the interface.

- **media-sfp**
  Specifies the settings for an SFP (pluggable) interface. Note that you use this option only with a combo port to specify the media type for the SFP interface, when it is not the preferred port.
- **mtu**
  Displays the Maximum Transmission Unit (MTU) of the interface, which is the maximum number of bytes in a frame without IP fragmentation.
- **name**
  Specifies an interface name, for example **3.1**, where **3** is the physical slot number holding the network interface hardware and **1** is the physical port number of that interface on that hardware. Another example is **mgmt**, the name given to the management interface.
- **no-mgmt**
  Ensures that no changes are made to the **mgmt** interfaces when **all** is specified. This is especially convenient when disabling all traffic interfaces using the **disabled** command.
- **[pending | not-pending]**
  Pending indicates that the slot with which the interface is associated does not contain a blade. **Not-pending** indicates that the slot with which the interface is associated is not a cluster member. The default value is pending.
- **prefer-port**
  Indicates which side of a combo port the interface uses, if both sides of the port have the potential for external links. The default value is **sfp**. Do not use this option for non-combo ports.
- **regex**
  Displays the items that match the regular expression. The regular expression must be preceded by an at sign (@[regular expression]) to indicate that the identifier is a regular expression. See **help regex** for a description of regular expression syntax.
- **sflow**
  Specifies sFlow settings for the interface:
  - **poll-interval**
    Specifies the maximum interval in seconds between two pollings. The default value is **0**. To enable this setting, you must also set the **poll-interval-global** setting to **no**.
  - **poll-interval-global**
    Specifies whether the global interface poll-interval setting, which is available under **sys sflow global-settings** module, overrides the object-level poll-interval setting. The default value is **yes**.
    The available values are:
    - **no**
      Specifies to use the object-level poll-interval setting.
    - **yes**
      Specifies to use the global interface poll-interval setting.

- **serial**
  Displays the serial number of the pluggable unit on an interface. It is only available on a SFP/SFP+/XFP/QSFP+ unit.
- **stp**
  Enables or disables STP. If you disable STP, no STP, RSTP, or MSTP packets are transmitted or received on the interface or trunk, and spanning tree has no control over forwarding or learning on the port or the trunk. The default value is **enabled**.
- **stp-auto-edge-port**
  Sets the STP automatic edge port detection for the interface. The default value is **enabled**. When STP automatic edge port detection is set to **enabled** on an interface, the system monitors the interface for incoming STP, RSTP, or MSTP packets. If no such packets are received for a sufficient period of time (about three seconds), the interface is automatically given edge port status. When automatic edge port detection is set to **disabled** on an interface, the system does not automatically give the interface the edge port status. Any STP setting set on a per-interface basis applies to all spanning tree instances.
- **stp-edge-port**
  Sets STP edge port detection. The default value is **true**.
- **stp-link-type**
  Specifies the STP link type for the interface. The default value is **auto**.
  The spanning tree system includes important optimizations that can only be used on point-to-point links. That is, on links that connect just two bridges. If these optimizations are used on shared links, incorrect or unstable behavior may result. By default, the implementation assumes that full-duplex links are point-to-point and that half-duplex links are shared.
  The options are:
  - **auto**
    Specifies that the system determines the spanning tree link type, which is based on the duplex setting.
  - **p2p**
    Specifies that the system uses the optimizations for point-to-point spanning tree links. Point-to-point links connect only two spanning tree bridges.
  - **shared**
    Specifies that the system uses the optimizations for shared spanning tree links. Shared links connect two or more spanning tree bridges.
- **stp-reset**
  Resets STP, which forces a migration check.
- **qinq-ethertype**
  Specifies the ether-type value used for the packets handled on this port when it is a member in a QinQ vlan. The ether-type can be set to

any string containing a valid hexadecimal 16 bits number, or any of the well known ether-types: **0x8100**, **0x9100**, **0x88a8**. Default value is set to **0x8100**.

- **if-index**
  Displays the index assigned to this interface. It is a unique identifier assigned for all objects displayed in the SNMP IF-MIB.
- **vendor**
  Displays the name of the vendor of the pluggable unit on an interface. It is only available on a SFP/SFP+/XFP/QSFP+ unit.

See Also

edit, glob, *list*, *modify*, regex, *reset-stats*, *show*, *tmsh*

interface-cos

Displays and resets COS (Class of Service) related statistics for the interfaces.

Syntax

Display cos related statistics within the **net** module using the following syntax.

Modify

```
reset-stats interface-cos
```

Display

```
show interface-cos
    (default | exa | gig | kil | meg | peta | raw | tera | yotta | zetta)
    global
```

Description

You can use the **interface-cos** component to display COS related stattics, including pkts out and bits out for all 8 COS queue.

Examples

show interface-cos

Displays interface COS related statistics for the system.

For information about the command **reset-stats**, see **help reset-stats**.

See Also

reset-stats, *show*,

ndp

Configures IPv6-to-Ethernet neighbor discovery display and control.

Syntax

Configure the **ndp** component within the **net** module using the syntax in the following sections.

Create/Modify

```
create ndp [name]
    description [string]
    ip-address [ip address]
    mac-address [MAC address]
modify ndp [name]
    description [string]
    mac-address [MAC address]
edit ndp [ [ [name] | [glob] | [regex] ] ... ]
    all-properties
    non-default-properties
```

Display

```
list ndp
list ndp [ [ [name] | [glob] | [regex] ] ... ]
show running-config ndp
show running-config ndp
  [ [ [name] | [glob] | [regex] ] ... ]
    all-properties
    non-default-properties
    one-line
show ndp
show ndp [ [ [name] | [glob] | [regex] ] ... ]
    [all | dynamic | field-fmt | static]
```

Delete

```
delete ndp [ [all]| [name]... ]
```

Description

Configures the IPv6-to-Ethernet address translation tables used by the IPv6 neighbor discovery protocol.

Examples

create ndp myNdp ip-address fec0:f515::c001 mac-address 00:0B:DB:3F:F6:57

Maps the IPv6 address, **fec0:f515::c001**, to the MAC address, **00:0B:DB:3F:F6:57**, and the name of this entry is myNdp. Alternatively, the address can be used as the name, like the following example.

create ndp fec0:f515::c001 mac-address 00:0B:DB:3F:F6:57

Maps the IPv6 address, **fec0:f515::c001**, to the MAC address, **00:0B:DB:3F:F6:57**.

show ndp

Displays all static and dynamic IPv6 address-to-MAC address mappings.

Options

- **ip-address**
  The IP address that is to be mapped. This is optional, and if not present, the name needs to be a string that represents a valid IP address.
- **description**
  User defined description.
- **dynamic**
  Displays dynamic IPv6 address-to-MAC address mapping.
- **glob**
  Displays the items that match the **glob** expression. See **help glob** for a description of **glob** expression syntax.
- **ip-address**
  The IP address that is to be mapped. This is optional, and if not present, the name needs to be a string that represents a valid IP address.
- **mac-address**
  Specifies a 6-byte Ethernet address in hexadecimal colon notation that is not case-sensitive, for example, **00:0b:09:88:00:9a**.
- **regex**
  Displays the items that match the regular expression. The regular expression must be preceded by an at sign (@[regular expression]) to indicate that the identifier is a regular expression. See **help regex** for a description of regular expression syntax.
- **static**
  Displays static IPv6 address-to-MAC address mapping.

See Also

create, *delete*, *edit*, glob, *list*, *modify*, regex, *show*, *tmsh*

packet-filter

Configures packet filter rules.

Syntax

Configure the **packet-filter** component within the **net** module using the syntax in the following sections.

Create/Modify

```
create packet-filter [name]
modify packet-filter [name]
    action [accept | continue | discard | reject]
    app-service [[string] | none]
    description [string]
    logging [enabled | disabled]
    order [integer]
    rate-class [name]
    rule "[BPF expression]"
    vlan [name]
edit packet-filter [ [ [name] | [glob] | [regex] ] ... ]
    all-properties
    non-default-properties
reset-stats packet-filter
reset-stats packet-filter
  [ [ [name] | [glob] | [regex] ] ... ]
```

Display

```
list packet-filter
list packet-filter
  [ [ [name] | [glob] | [regex] ] ... ]
show running-config packet-filter
show running-config packet-filter
  [ [ [name] | [glob] | [regex] ] ... ]
    all-properties
    non-default-properties
    one-line
show packet-filter
show packet-filter [ [ [name] | [glob] | [regex] ] ... ]
    (default | exa | gig | kil | meg | peta | raw | tera | yotta | zetta)
    field-fmt
```

Delete

```
delete packet-filter [ all | [name] ]
```

Description

You can use the **packet-filter** component to create a layer of security for the traffic management system using packet filter rules.

The BIG-IP® system packet filters are based on the Berkeley Software Design Packet Filter (BPF) architecture. Packet filter rules are composed of four mandatory attributes and three optional attributes. The mandatory attributes are **name**, **order**, **action**, and **rule**. The optional attributes are **vlan**, **logging**, and **rate-class**. The rule attribute you choose defines the BPF script to match for the rule.

Important

By default, packet filtering is disabled. You must enable packet filtering using the Configuration utility. For more information, see the TMOS® Management Guide for BIG-IP® Systems.

Examples

You can create a set of rules that specify what incoming traffic you want the system to accept and how to accept it. See the examples following.

- Example 1: Block spoofed addresses
  This example prevents private IP addresses from being accepted on a public VLAN. This is a way of ensuring that no one can spoof private IP addresses through the external VLAN of the system. In this example, the system logs when this happens:

```
create packet-filter spoof_blocker {
   order 5
   action discard
   vlan external
   logging enabled
   rule " (src net 172.19.255.0/24) "
}
```

- Example 2: Allow restricted management access
  You can provide restricted SSH and HTTPS access to the traffic management system for management purposes, and keep a log of that access. **Note:** This not the same management access you can get through the management port/interface (mgmt); that interface is not affected by any packet filter configuration, and if that is the only way you want to allow access to your system, this configuration is not necessary.
  In the first rule shown below, SSH is allowed access from a single fixed-address administrative workstation, and each access is logged. In the subsequent rule, browser-based Configuration utility access is allowed from two fixed-address administrative workstations; however, access is not logged.

```
create packet-filter management_ssh {
     order 10
     action accept
     logging enabled
     rule " (proto TCP) and (src host 172.19.254.10)
and
            (dst port 22) "
}
```

```
create packet-filter management_gui {
     order 15
     action accept
     rule " (proto TCP) and (src host 172.19.254.2 or
            src host 172.19.254.10) and (dst port 443)
"
}
```

- Example 3: Allow access to all virtual servers
  In this final example, you can verify that all of the virtual servers in your configuration are reachable from the public network. This is critical if you have decided to use a default-deny policy. This example also shows how to rate shape all traffic to the virtual server IP address with a default rate class (that can be overridden by individual virtual servers or iRules® later).

◆ Note

This example has a single virtual server IP, and it does not matter what port traffic is destined for. If you want to be more specific, you can specify each service port, as well (for example, HTTP, FTP, telnet).

```
create packet-filter virtuals {
      order 20
      action accept
      vlan external
      rate class root
      rule " ( dst host 172.19.254.80 ) "
 }
```

Options

You can use these options with the **packet-filter** component to create packet filter rules:

- **action**
  Specifies how the system handles a packet that matches the criteria in the packet filter rule. There is no default; you must specify a value when you create a packet filter rule.
  The possible values are:
  - **accept**
    Indicates that the system accepts the packet, and stops processing additional packet filter rules, if there are any.
  - **continue**
    Indicates that the system acknowledges the packet for logging or statistical purposes, but makes no decision on how to handle the packet. The system continues to evaluate traffic matching a rule with the Continue action, starting with the next packet filter rule in the list.
  - **discard**
    Indicates that the system drops the packet, and stops processing additional packet filter rules, if there are any.

- **reject**
  Indicates that the system drops the packet, and also sends a reject packet to the sender, indicating that the packet was refused.

- **app-service**
  Specifies the name of the application service to which the object belongs. The default value is **none**. **Note:** If the **strict-updates** option is **enabled** on the application service that owns the object, you cannot modify or delete the object. Only the application service can modify or delete the object.
- **description**
  User defined description.
- **glob**
  Displays the items that match the **glob** expression. See **help glob** for a description of **glob** expression syntax.
- **logging**
  Enables or disables packet filter logging. If you omit this value, no logging is performed.
- **name**
  Specifies a unique name for the component. This option is required for the commands **create**, **delete**, and **modify**.
- **order**
  Specifies a sort order greater than **0** (zero). No two rules may have the same sort order. There is a single, global list of rules. Each rule in the list has a relative integer **order**. The system first evaluates the rule with the lowest **order** value, and then evaluates all other rules based on ascent of the **order** value assigned to each rule.
  For example, if there are 5 rules, numbered 500, 100, 300, 200, 201; the rule evaluation order is 100, 200, 201, 300, 500.
  The system compares each packet to be filtered against the list of rules in sequence, starting with the first. Evaluation of the rule list stops on the first match that has an action of **accept**, **discard** or **reject**. A match on a rule with an action of **none** does not stop further evaluation of the rule list; the system updates the statistics count and generates a log if the rule indicates it, but otherwise rule processing continues with the next rule in the list.
  F5 Networks recommends that you sequence rules for effect and efficiency; generally this means:
  -- Assign the lowest order to more specific rules, so that the system will evaluate those rules first.
  -- The system evaluates one expression with multiple criteria more efficiently than multiple expressions each with a single criterion.
  This option is required.
- **rate-class**
  Specifies the name of a rate class. The value is the name of any existing rate class. If omitted, no rate filter is applied.

- **regex**
  Displays the items that match the regular expression. The regular expression must be preceded by an at sign (@[regular expression]) to indicate that the identifier is a regular expression. See **help regex** for a description of regular expression syntax.
- **rule**
  Specifies the BPF expression to match. The rule is mandatory, however you can leave it empty. If empty, the packet filter rule matches all packets.
- **vlan**
  Specifies the VLAN to which the packet filter rule applies. The value for this option is any VLAN name currently in existence. If you omit this value, the rule applies to all VLANs. If you do not provide a VLAN name when you create a packet-filter, the rule applies to all VLANs.

See Also

create, *delete*, *edit*, glob, *list*, *virtual*, *modify*, *packet-filter-trusted*, *vlan*, *vlan-group*, regex, *reset-stats*, *show*, *tmsh*

packet-filter-trusted

Modifies or displays trusted allow lists for packet filters.

Syntax

Configure the **packet-filter-trusted** component within the **net** module using the syntax in the following sections.

Modify

```
modify packet-filter-trusted
    description [string]
    ip-addresses none
    ip-addresses
      [add | delete | replace-all-with] {
        [ip address ... ]
    }
    mac-addresses none
    mac-addresses
      [ add | delete | replace-all-with] ] {
        [MAC address ...]
    }
    vlans none
    vlans
      [add | delete | replace-all-with] ] {
        [vlan name ... ]
    }
edit packet-filter-trusted
```

Display

```
list packet-filter-trusted
show running-config packet-filter-trusted
    all-properties
    non-default-properties
    one-line
```

Description

Use the **packet-filter-trusted** component to create a layer of security for the traffic management system using trusted allow lists.

Trusted allow lists are lists of IP addresses, MAC addresses, and VLANs that are exempt from packet filter rules.

Important

By default, packet filtering is disabled. You must enable packet filtering using the Configuration utility. For more information, see the TMOS® Management Guide for BIG-IP® Systems.

Example

Creates a trusted allow list that allows anything listed to bypass the packet filter.

In the following example, you have an administrative laptop that you want to have unrestricted access to the traffic management system. This is a laptop, and therefore it might have a different IP address from time to time. One way to solve the problem is to add a trusted MAC address. This trusted allow list example shows the laptop MAC address as 00:02:3F:3E:2F:FE. Now the laptop can access the traffic management system regardless of what address it boots with or to which VLAN it is connected, as long as it is on the same physical segment as the traffic management system.

Also in this example, the traffic management system is configured for basic firewalling of the private/internal network. This example shows a way to filter incoming traffic and allow outgoing traffic to be unrestricted. To do this, you add trusted VLANs that represent all traffic that originated on the internal network. Another way to do this is to use trusted IP addresses instead, for example, **192.168.26.0/24**.

```
modify packet-filter-trusted {
  vlans add { internal1 internal2 }
  mac-addresses add { 00:02:3F:3E:2F:FE }
}
```

Options

- **description**
  User defined description.
- **ip-addresses**
  Specifies a list of source IP addresses. Any traffic matching a source IP address in the list is automatically allowed. This simplifies configuration of the packet filter to allow trusted internal traffic to be passed from VLAN to VLAN without a filter rule, including out to the Internet. Processing of traffic by this option occurs before rule list evaluation, making it impossible to override this option and mask out (block) certain types of traffic with a packet filter rule. This option is empty by default.
- **mac-addresses**
  Specifies a list of MAC addresses. The system allows any traffic matching a MAC address in the source address list. This simplifies configuration of the packet filter to allow trusted internal traffic to be passed from VLAN to VLAN without a filter rule, including out to the Internet. Processing of traffic by this option occurs before rule list evaluation, making it impossible to override this option and mask out (block) certain types of traffic with a packet filter rule. This option is empty by default.
- **vlans**
  Specifies a list of ingress VLANs. Any traffic received on a VLAN that is on the ingress VLAN list is automatically allowed. This simplifies configuration of the packet filter to allow trusted internal traffic to be passed from VLAN to VLAN without a filter rule, including out to the

Internet. Processing of traffic by this option occurs before rule list evaluation, making it impossible to override this option and mask out (block) certain types of traffic with a packet filter rule. This option is empty by default.

See Also

edit, *list*, *virtual*, *modify*, *packet-filter*, *vlan*, *vlan-group*, *show*, *tmsh*

port-mirror

Configures interface (port) mirroring.

Syntax

Configure the **port-mirror** component within the **net** module using the syntax in the following sections.

Create/Modify

```
create port-mirror [interface_name]
modify port-mirror [interface_name]
    app-service [[string] | none]
    interfaces
      [add | delete | replace-all-with] {
        [interface_name ... ]
    }
    interfaces [default | none]
edit port-mirror [ [ [interface_name] | [glob] | [regex] ] ... ]
  all-properties
```

Display

```
list port-mirror
list port-mirror
  [ [ [interface_name] | [glob] | [regex] ] ... ]
show running-config port-mirror
show running-config port-mirror
  [ [ [interface_name] | [glob] | [regex] ] ... ]
    one-line
```

Delete

```
delete port-mirror [interface_name]
```

Description

You can use the **port-mirror** component to mirror traffic from interfaces on a blade to other interfaces on the same blade or another blade.

Examples

create port-mirror 1/1.1 interfaces add 1/1.2 1/1.3 1/1.4

Creates a port mirror from interface **1.1** on blade **1** to interfaces **1.2**, **1.3**, **1.4** on the same blade. The system mirrors traffic from interfaces 1.2, 1.3, and 1.4 on blade 1 to the interface 1.1 on the same blade.

modify port-mirror 1/1.1 interfaces delete 1/1.3 1/1.4

Deletes interfaces **1.3** and **1.4** on blade **1** from the existing port mirror **1/1.1** on the same blade.

Option

- **app-service**
  Specifies the name of the application service to which the object belongs. The default value is **none**. **Note:** If the **strict-updates** option is **enabled** on the application service that owns the object, you cannot modify or delete the object. Only the application service can modify or delete the object.
- **glob**
  Displays the items that match the **glob** expression. See **help glob** for a description of **glob** expression syntax.
- **interface_name**
  Specifies the name of the interface, for example, **1/1.1**.
- **regex**
  Displays the items that match the regular expression. The regular expression must be preceded by an at sign (@[regular expression]) to indicate that the identifier is a regular expression. See **help regex** for a description of regular expression syntax.

See Also

create, *delete*, *edit*, glob, *list*, *modify*, *interface*, regex, *show*, *tmsh*

route

Configures a route for traffic management.

Syntax

Configure the **route** component within the **net** module using the syntax in the following sections.

Create/Modify

```
create route [name | ip address/netmask | default | default-inet6]
modify route [name | ip address/netmask | default | default-inet6]
    blackhole
    description [string]
    gw [ip address]
    interface [name]
    mtu [integer]
    network [ip address/netmask]
    pool [name]
edit route
  [ [name | ip address/netmask | default | default-inet6] | [glob] | [regex] ] ... ]
    all-properties
    non-default-properties
```

Display

```
list route
list route
  [ [name | ip address/netmask | default | default-inet6] | [glob] | [regex] ] ... ]
show running-config route
show running-config route
  [ [name | ip address/netmask | default | default-inet6] | [glob] | [regex] ] ... ]
    all-properties
    mtu
    non-default-properties
    one-line
    partition
show route
show route
  [ [name | ip address/netmask | default | default-inet6] | [glob] | [regex] ] ... ]
    connected
    dynamic
    field-fmt
    lookup [ip address]
    static
```

Delete

```
delete route [name | ip address/netmask | default | default-inet6]
```

Description

You can configure routes for the system, including default routes.

Note that when you use the command **edit** to create a new route, by default the **gw** (gateway) option is set. If you do not want to use the **gw** option, remove that line of syntax in the editor.

Examples

create route myRoute3 network 12.12.4.0/24 interface external

Sets the route myRoute3 to the address **12.12.4.0/24** on the interface named **external**.

create route 12.12.3.0/24 gw 10.10.10.254

Sets the route to the subnet **12.12.3.0/24** whose gateway IP address is **10.10.10.254**.

create route default gw 10.10.10.254

Sets the default gateway IP address to **10.10.10.254**.

show route lookup myRoute

Displays the route that the system uses to reach the IP address **12.12.3.0**.

Options

Note: The options **blackhole**, **gw**, **interface**, and **pool** are mutually exclusive. You can use only one of these options at a time, and you must specify at least one of these options when configuring a route.

- **blackhole**
  Specifies that the system drops traffic that is addressed to the specified destination.
- **connected**
  Displays connected routes.
- **description**
  User defined description.
- **dynamic**
  Displays dynamic routes.
- **glob**
  Displays the items that match the **glob** expression. See **help glob** for a description of **glob** expression syntax.
- **gw**
  Specifies a gateway address for the system.
- **interface**
  Specifies the tunnel, VLAN or VLAN group to which the system sends traffic.

- **ip address/netmask**
  Specifies the destination subnet and mask using CIDR notation, such as **12.12.3.0/24**. You can also specify the keyword **default** or **default-inet6**.
- **lookup**
  Displays the route that the system uses to reach the specified IP address. You can specify only a single IP address with the **lookup** option.
- **mtu**
  Sets a specific maximum transition unit (MTU). If you set this option to **0** (zero), the system selects the appropriate MTU for the route, and does not display the MTUs.
- **network**
  Specifies the destination subnet and mask using CIDR notation, such as **12.12.3.0/24**. You can also specify the keyword **default** or **default-inet6**.
- **partition**
  Displays the administrative partition within which the route resides.
- **pool**
  Specifies a pool to which the system sends traffic. This allows the system to send traffic to multiple, load-balanced gateways.
- **regex**
  Displays the items that match the regular expression. The regular expression must be preceded by an at sign (@[regular expression]) to indicate that the identifier is a regular expression. See **help regex** for a description of regular expression syntax.
- **static**
  Displays static routes.

See Also

create, *delete*, *edit*, glob, *list*, *pool*, *modify*, *vlan*, *vlan-group*, regex, *show*, *tmsh*

route-domain

Configures route-domains for traffic management.

Syntax

Configure the **route-domain** component within the **net** module using the syntax in the following sections.

Create/Modify

```
create route-domain [ [name] | none]
    id [integer]
modify route-domain [name]
    app-service [[string] | none]
    bwc-policy [string]
    connection-limit [integer]
    description [string]
    flow-eviction-policy [ [eviction policy name] | none ]
    fw-enforced-policy [ [policy_name] | none ]
    fw-rules [add | delete | modify | replace-all-with] {
      [ [name] ] {
          action [accept | accept-decisively | drop | reject]
          description [string]
          destination {
            address-lists [add | default | delete | replace-all-with] {
              [address list names...]
            }
            address-lists none
            addresses [add | default | delete | replace-all-with] {
              [ [ip address] | [ip address/prefixlen] ]
            }
            addresses none
            port-lists [add | default | delete | replace-all-with] {
              [port list names...]
            }
            port-lists none
            ports [add | default | delete | none | replace-all-with] {
              [ [port] | [port1-port2] ]
            }
            ports none
          }
          icmp [add | delete | modify | replace-all-with] {
            [ [icmp_type] | icmp_type:icmp_code ] {
              description [string]
            }
          }
          icmp none
          ip-protocol [protocol name]
          irule [irule name]
          irule-sample-rate [integer]
          log [no | yes]
          place-after [first | last | [rule name]]
          place-before [first | last | [rule name]]
          rule-list [rule list name]
          schedule [schedule name]
          source {
```

```
            address-lists [add | default | delete | replace-all-with] {
              [address list names...]
            }
            address-lists none
            addresses [add | default | delete | replace-all-with] {
              [ [ip address] | [ip_address/prefixlen] ]
            }
            addresses none
            port-lists [add | default | delete | replace-all-with] {
              [port list names...]
            }
            port-lists none
            ports [add | default | delete | replace-all-with] {
              [ [port] | [port1-port2] ]
            }
            ports none
            vlans [add | default | delete | replace-all-with] {
              [vlan names...]
            }
            vlans none
          }
          status [disabled | enabled | scheduled]
      }
    }
    fw-rules none
    fw-staged-policy [ [policy_name] | none ]
    id [integer]
    parent [ [name] | none]
    strict [disabled | enabled]
    routing-protocol
      [add | delete | replace-all-with] {
        [protocol name] ...
    }
    vlans
      [add | delete | replace-all-with] {
        [vlan name] ...
    }
edit route-domain [ [name] | [glob] | [regex] ] ... ]
    all-properties
    non-default-properties
reset-stats route-domain [name]
  fw-enforced-policy-rules { [rule name] }
  fw-rules  { [rule name] }
  fw-staged-policy-rules  { [rule name] }
options:
  ip-intelligence-categories
```

Display

```
list route-domain
list route-domain [ [name] | [glob] | [regex] ] ... ]
show running-config route-domain
show running-config route-domain
  [ [name] | [glob] | [regex] ] ... ]
    all-properties
    one-line
    non-default-properties
show route-domain [ [ [name] | [glob] | [regex] ] ... ]
    ip-intelligence-categories
```

Delete

```
delete route-domain [name]
```

Description

Using route domains, you can assign the same IP address to more than one device on a network, as long as each instance of the IP address resides in a separate routing domain.

Examples

create route-domain myRouteDomain id 1 vlans add { my_vlan }

Creates a route domain named myRouteDomain with an ID of 1 that includes **my_vlan**.

list route-domain all-properties

Displays all properties of all route domains.

Options

- **app-service**
  Specifies the name of the application service to which the object belongs. The default value is **none**. **Note:** If the **strict-updates** option is **enabled** on the application service that owns the object, you cannot modify or delete the object. Only the application service can modify or delete the object.
- **bwc-policy**
  Configures the bandwidth control policy for the route-domain. If set, it will enforce a throughput policy for incoming network traffic.
- **connection-limit**
  Configures the connection limit for the route domain. If set to a value other than zero, this specifies the total number of open connections allowed on this route domain. The default value is **0**, unlimited.
- **description**
  User defined description.
- **id**
  Specifies a unique numeric identifier for the route-domain. This option is required during creation; it may not be modified once set.
- **flow-eviction-policy**
  Specifies a flow eviction policy for the route domain to use, to select which flows to evict when the number of connections approaches the connection limit on the route domain. The default value is **none**.

- **fw-enforced-policy**
  Specifies an enforced firewall policy. **fw-enforced-policy** rules are enforced on a route-domain as if the policy rules were explicitly defined in the route-domain's **fw-rules**. Either **fw-rules** or **fw-enforced-policy** can be configured on a route-domain, not both of them.
- **fw-enforced-policy-rules**
  Specifies firewall rules enforced on **net route-domain** via referenced **fw-enforced-policy**.
- **fw-rules**
  Adds, deletes, or replaces a firewall rule. **net route-domain** rules are checked when a packet is received.
  - **action**
    Specifies the action that the system takes when a rule is matched.
    - **accept**
      Specifies that the current packet should be accepted. The packet will be compared to rules in the next appropriate context (**net self-ip** or **ltm virtual**).
    - **accept-decisively**
      Specifies that the current packet should be accepted and that packet will not be compared to any other firewall rules in any other context.
    - **drop**
      Specifies that the current packet should be silently dropped. Nothing is sent back to the packet source. The packet is not compared to any other firewall rules.
    - **reject**
      Specifies that the current packet should be dropped. For TCP based protocols a TCP reset is sent to the source. For other protocols **reject** is equivalent to **drop**.
  - **description**
    User defined description.
  - **destination**
    - **address-lists**
      Specifies a list of address lists (see **security firewall address-list**) against which the packet will be compared.
    - **addresses**
      Specifies a list of addresses and networks against which the packet will be compared.
    - **port-lists**
      Specifies a list of port lists (see **security firewall port-list**) against which the packet will be compared.
    - **ports**
      Specifies a list of ports and port ranges against which the packet will be compared.

- **icmp**
  Specifies a list of ICMP types and codes against which the packet will be compared. The standard integer identifiers are used to specify an ICMP type Example: 3 is destination unreachable and 3:1 is destination unreachable with a code of host unreachable. The list of ICMP types and codes can be found here http://www.iana.org/assignments/icmp-parameters/icmp-parameters.xml.
- **ip-protocol**
  Specifies the IP protocol against which the packet will be compared.
- **irule**
  Specifies the name of the iRule that will be triggered when a packet matches this firewall rule. The firewall rule match raises a FLOW_INIT iRule event.
- **irule-sample-rate**
  Specifies the rate at which an iRule specified by **irule** option will be triggered when a packet matches this firewall rule. The rate is an integer value in the range 0-65535 and specifies how many packets must match this firewall rule before the iRule is triggered. The default value is 1 and causes the iRule to be triggered for every packet that matches this firewall rule. A value of 0 disables iRule triggering.
- **log**
  Specifies whether the packet will be logged if it matches the rule. Logging must also be enabled in the **security log profile global-network** configuration. Note that the statistics counter is always incremented when a packet matches a rule.
- **place-after**
  Specifies that a new rule should be placed after another rule, **first** or **last**. If individual rules are being added (as opposed to specifying **replace-all-with**) then **place-before** or **place-after** must be specified.
- **place-before**
  Specifies that a new rule should be placed before another rule, **first** or **last**. If individual rules are being added (as opposed to specifying **replace-all-with**) then **place-before** or **place-after** must be specified.
- **rule-list**
  Specifies a list of rules to evaluate. See **security firewall rule-list**. If a **rule-list** is specified then only the **schedule** and **status** properties effect the rule.
- **schedule**
  Specifies a schedule for the rule. See **security firewall schedule**. If the rule refers to a **rule-list** the **rule-list** will be enabled according to the schedule. When the **rule list** is enabled, the schedules defined within the **rule-list** will be honored.
- **source**

  - **address-lists**
    Specifies a list of address lists (see **security firewall address-list**) against which the packet will be compared.

- **addresses**
  Specifies a list of addresses and networks against which the packet will be compared.
- **port-lists**
  Specifies a list of port lists (see **security firewall port-list**) against which the packet will be compared.
- **ports**
  Specifies a list of ports and port ranges against which the packet will be compared.
- **vlans**
  Specifies a list of vlans, vlan groups and tunnels against which the packet will be compared.

- **status**
  Specifies whether the rule is **enabled**, **disabled** or **scheduled**. A rule that is **enabled** is always checked. A rule that is **disabled** is never checked. A rule that is **scheduled** is checked according to the corresponding schedule configuration. A rule that is **scheduled** must have an associated schedule configuration.

◆ **fw-staged-policy**
Specifies a staged firewall policy. **fw-staged-policy** rules are not enforced while all the visibility aspects namely statistics, reporting and logging function as if the **fw-staged-policy** rules were enforced on a route-domain.

◆ **fw-staged-policy-rules**
Specifies firewall rules staged on **net route-domain** via referenced **fw-staged-policy**.

◆ **parent**
Specifies the route domain the system searches when it cannot find a route in the configured domain. The default value is **None**.
If you specify a **parent**, during route table lookup, if the system cannot find a route in the current route domain, the system searches routes in the parent route domain. If no route is found in the parent route domain, the system searches the parent route domain's parent, and so on, until the system finds either a match or a **parent** with a value of **None**. For example, if **rd_1** has a **parent** of **rd_0** (in this example, route domain **rd_0** has a **parent** of **None**), and you include **vlan_a** in **rd_1**, when requests arrive for **vlan_a**, the system looks in **rd_1** for a route for the specified destination. If no route is found, the system searches route domain 0. If it still cannot find a route, the request for **vlan_a** fails. If, using the same example, you set the **parent** to **None**, under the same conditions, the system looks in **rd_1**, and if it cannot find a matching route, the system refrains from searching any other route domain, the request for **vlan_a** fails.

◆ **regex**
Displays the items that match the regular expression. The regular expression must be preceded by an at sign (@[regular expression]) to indicate that the identifier is a regular expression. See **help regex** for a description of regular expression syntax.

- **strict**
  Specifies whether the system allows a connection to span route domains. The default value is **enabled**.

◆ Note

When you enable this option, the system may find invalid iRules® that passed validation.

- **routing-protocol**
  Specifies routing protocols, by name, for the system to use in the route domain. The default value is **none**. Dynamic routing must be licensed to use this option.
- **vlans**
  Specifies VLANs, by name, for the system to use in the route domain. The default value is **none**.
- **ip-intelligence-categories**
  Used to show/ reset statistics on IP intelligence white/ black lists categories.

See Also

create, *delete*, *edit*, glob, *list*, *modify*, *vlan*, *vlan-group*, regex, *show*, *tmsh*, *bwc-policy*

router-advertisement

Configures IPv6 prefixes for router advertisement on a VLAN.

Syntax

Modify the **router-advertisement** component within the **net** module using the syntax shown in the following sections.

Create/Modify

```
create router-advertisement [name]
modify router-advertisement [name]
    app-service [[string] | none]
    current-hop-limit [integer]
    description [string]
    disabled | enabled
    max-interval [integer]
    min-interval [integer]
    mtu [integer]
    no-other-config | other-config
    prefixes
      [add | delete | modify | replace-all-with] {
        [name] ... {
          app-service [[string] | none]
          autonomous | not-autonomous
          description [string]
          on-link | not-on-link
          preferred-lifetime [integer]
          prefix [ip address]
          prefix-length [integer]
          valid-lifetime [integer]
        }
    }
    reachable-time [integer]
    retransmit-timer [integer]
    router-lifetime [integer]
    unmanaged | managed
    vlan [name]
edit router-advertisement [ [ [name] | [glob] | [regex] ] ... ]
    all-properties
    non-default-properties
```

Display

```
list router-advertisement
list router-advertisement [ [ [name] | [glob] | [regex] ] ... ]
show running-config router-advertisement
show running-config router-advertisement
  [ [ [name] | [glob] | [regex] ] ... ]
    all-properties
    non-default-properties
    one-line
```

Delete

```
delete router-advertisement [name]
```

Description

Router advertisements are part of the configuration of BIG-IP® network components. When creating a router advertisement, you must specify a VLAN on the command line.

Examples

create router-advertisement my_ra vlan my_vlan

Creates the router advertisement **my_ra** that includes the VLAN **my_vlan**.

delete router-advertisement my_ra

Deletes the router advertisement named **my_ra** and all associated prefixes.

Options

Note the following information regarding options for the **router-advertisement** component:

- The options **disabled** and **enabled** are mutually exclusive.
- The options **no-other-config** and **other-config** are mutually exclusive.
- The options **unmanaged** and **managed** are mutually exclusive.
- The options **autonomous** and **not-autonomous** are mutually exclusive.
- The options **on-link** and **not-on-link** are mutually exclusive.
- **app-service**
  Specifies the name of the application service to which the object belongs. The default value is **none**. **Note:** If the **strict-updates** option is **enabled** on the application service that owns the object, you cannot modify or delete the object. Only the application service can modify or delete the object.
- **autonomous**
  Indicates that the Autonomous Flag field in the prefix information option be set to **1**. The default value is **1**.
- **current-hop-limit**
  Defines the hop limit sent in the router advertisement. The default value is **0** (zero).

- **description**
  User defined description.
- **disabled**
  Disables router advertisement for the VLAN. This is the default.
- **enabled**
  Enables router advertisement for the VLAN.
- **glob**
  Displays the items that match the **glob** expression. See **help glob** for a description of **glob** expression syntax.
- **managed**
  Indicates that the Managed address configuration flag field in the router advertisement be set to **1**.
- **max-interval**
  Specifies the maximum time allowed between sending unsolicited multicast Router Advertisements from the interface, in seconds. The default value is **600**.
- **min-interval**
  Specifies, in seconds, the minimum time allowed between sending unsolicited multicast Router Advertisements from the interface. The default value is **200**.
- **mtu**
  Sets a specific maximum transition unit (MTU) for the VLAN. The default value is **0** (zero).
- **name**
  Specifies a unique name for the component. This option is required for the **create**, **delete**, and **modify** commands.
- **no-other-config**
  Indicates that the Other Configuration flag field in the router advertisement be set to **0** (zero). The default value is **0** zero.
- **not-autonomous**
  Indicates that the Autonomous flag field in the prefix information option be set to **0** (zero).
- **not-on-link**
  Indicates that the on-link flag field in the prefix information option be set to **0** (zero).
- **on-link**
  Indicates that the on-link flag field in the prefix information option be set to **1**. The default value is **1**.
- **other-config**
  Indicates that the Other Configuration flag field in the router advertisement be set to **1**.
- **preferred-lifetime**
  Specifies, in seconds, the value for the Preferred Lifetime field in the prefix information option. The default value is **604800**.
- **prefix**
  Specifies the prefix for the prefix information option.

- **prefix-length**
  Specifies the length of the prefix for the prefix information option.
- **prefixes**
  Specifies the objects that hold the prefix specific information for the router advertisement.
- **reachable-time**
  Specifies the value to be used for the Reachable Time field in the Router Advertisement. The default value is **0** (zero).
- **regex**
  Displays the items that match the regular expression. The regular expression must be preceded by an at sign (@[regular expression]) to indicate that the identifier is a regular expression. See **help regex** for a description of regular expression syntax.
- **retransmit-timer**
  Specifies the value to be used for the Retransmit Timer field in the Router Advertisement. The default value is **0** (zero).
- **router**
  Specifies that the router advertisement acts as a router for the VLAN.
- **router-lifetime**
  Specifies the value to be used for the Router Lifetime field in the Router Advertisement. The default value is **1800**.
- **unmanaged**
  Specifies that the Managed address configuration flag field in the router advertisement be set to **0** (zero). The default value is **0** (zero).
- **valid-lifetime**
  Specifies, in seconds, the value for the Valid Lifetime field in the prefix information option. The default value is **2592000**.

See Also

create, *delete*, *edit*, glob, *list*, *modify*, *vlan*, regex, *show*, *tmsh*

rst-cause

Displays and Reset TCP/IP Reset Cause Statistics

Syntax

Display and Reset the **rst-cause** component within the **net** module using the syntax in the following section.

Modify

```
reset-stats rst-cause
```

Display

```
show rst-cause
    (default | field-fmt)
```

Description

You can use the **rst-cause** component to display and reset TCP/IP reset cause statistics. This will help to debug the reason for TCP/IP reset.

Options

For information about the options that you can use with the command **show**, see **help show**.

See Also

reset-stats, *show*, *tmsh*

self

Configures a self IP address for a VLAN.

Syntax

Modify the **self** component within the **net** module using the syntax shown in the following sections.

Create/Modify

```
create self [name]
modify self [name]
   address [ip address/netmask]
   allow-service [all | default | none]
   allow-service
     [add | delete | replace-all-with] {
       [protocol:port] ...
   }
   app-service [[string] | none]
   description [string]
   fw-enforced-policy [ [policy_name] | none ]
   fw-rules [add | delete | modify | replace-all-with] {
     [ [name] ] {
        action [accept | drop | reject]
        description [string]
        destination {
          address-lists [add | default | delete | replace-all-with] {
            [address list names...]
          }
          address-lists none
          addresses [add | default | delete | replace-all-with] {
            [ [ip address] | [ip address/prefixlen] ]
          }
          addresses none
          port-lists [add | default | delete | replace-all-with] {
            [port list names...]
          }
          port-lists none
          ports [add | default | delete | none | replace-all-with] {
            [ [port] | [port1-port2] ]
          }
          ports none
        }
        icmp [add | delete | modify | replace-all-with] {
          [ [icmp_type] | icmp_type:icmp_code ] {
            description [string]
          }
        }
        icmp none
        ip-protocol [protocol name]
        irule [irule name]
        irule-sample-rate [integer]
        log [no | yes]
        place-after [first | last | [rule name]]
        place-before [first | last | [rule name]]
        rule-list [rule list name]
```

```
        schedule [schedule name]
        source {
          address-lists [add | default | delete | replace-all-with] {
            [address list names...]
          }
          address-lists none
          addresses [add | default | delete | replace-all-with] {
            [ [ip address] | [ip_address/prefixlen] ]
          }
          addresses none
          port-lists [add | default | delete | replace-all-with] {
            [port list names...]
          }
          port-lists none
          ports [add | default | delete | replace-all-with] {
            [ [port] | [port1-port2] ]
          }
          ports none
          vlans [add | default | delete | replace-all-with] {
            [vlan names...]
          }
          vlans none
        }
        status [disabled | enabled | scheduled]
      }
    }
    fw-rules none
    fw-staged-policy [ [policy_name] | none ]
    traffic-group [[string] | default | non-default | none]
    vlan [name]
  edit self [
    [ [name] | [glob] | [regex] ] ... ]
      all-properties
      non-default-properties
  reset-stats self [ [ [name] | [glob] | [regex] ] ... ]
    fw-enforced-policy-rules { [rule name] }
    fw-rules  { [rule name] }
    fw-staged-policy-rules  { [rule name] }
  mv self [ [[source-name] [destination-name]] | [[name] to-folder [folder-name]] |
  [[name...name] to-folder [folder-name]] ]
      to-folder
```

Display

```
list self
list self
  [ [ [name] | [glob] | [regex] ] ... ]
show running-config self
show running-config self
  [ [ [name] | [glob] | [regex] ] ... ]
   all-properties
   non-default-properties
   one-line
```

Delete

```
delete self [name]
```

Description

A self IP address is an IP address that is assigned to the system. Self IP addresses are part of the configuration of the BIG-IP® network components. You must define at least one self IP address for each VLAN.

Examples

create self mySelf address 10.10.10.24/16 vlan internal

Adds the self IP address **10.10.10.24** to the VLAN named **internal**. This entry is named mySelf. Alternatively, the name can encompass the IP address and mask fields, like the following example.

create self 10.10.10.24/16 vlan internal

Adds the self IP address **10.10.10.24** to the VLAN named **internal**.

modify self 10.1.1.1/16 vlan external traffic-group /Common/traffic-group-1

Enables a floating IP address on the external VLAN. The **traffic-group** option makes this virtual address available to whichever device is active on the given traffic-group. In other words, when the standby device becomes the active device for that traffic-group, it uses this virtual address. Only one of the devices in the traffic-group can use the IP address at any given time.

mv /net self /Common/10.10.10.15/24 /Common/myselfIP2

Moves/Renames the **Self IP** from **10.10.10.15/24** to **myselfIP2**.

◆ Note

If you wish to change the name of the self IP, you may use a name that is the same as the IP Address or a name that does not represent a different IP Address than the one configured. If using prefix-length adornment on the name, it must match the existing prefix-length/netmask for the self IP.

Please refer to the **mv** manual page for additional examples on how to use the mv command.

Options

- **allow-service**
  Specifies the type of protocol/service that the VLAN handles. If you use this property to allow SSH, HTTP, and/or HTTPS service, administrators can use this self-IP address to log into the BIG-IP system; this makes the current self-IP available as a management-IP address on the VLAN.
  The options are:
  - **add**
    Adds the specified protocol/service to the VLAN.
  - **all**
    Specifies that the VLAN handles all protocols/services.

- **app-service**
  Specifies the name of the application service to which the object belongs. The default value is **none**. **Note:** If the **strict-updates** option is **enabled** on the application service that owns the object, you cannot modify or delete the object. Only the application service can modify or delete the object.
- **default**
  Specifies that the system uses a pre-defined set of network protocols/services that are commonly required for BIG-IP deployment. You can customize this set of services with the *self-allow* component.
  This is not the default for the **allow-service** property; **none**, described below, is the actual default.
- **delete**
  Removes the specified protocol/service from the VLAN.
- **none**
  Specifies that the VLAN handles no protocols/services. This is the default setting for a self IP address.
- **replace-all-with**
  Replaces the current protocol/service that the VLAN handles with the specified protocol/service.

◆ **address**
Specifies the IP address and netmask to be assigned to the system. This is an optional field. If not specified, the name of the entry must appear in the format [ip address/mask].

◆ **description**
User-defined description.

◆ **floating**
Read-only property based on the **traffic-group**. A floating self IP address is a self IP address for a VLAN that serves as a shared address by all devices of a BIG-IP traffic-group.

◆ **fw-enforced-policy**
Specifies an enforced firewall policy. **fw-enforced-policy** rules are enforced on a self IP address as if the policy rules were explicitly defined in the self IP address's **fw-rules**. Either **fw-rules** or **fw-enforced-policy** can be configured on a self IP address, not both of them.

◆ **fw-enforced-policy-rules**
Specifies firewall rules enforced on **net self** via referenced **fw-enforced-policy**.

◆ **fw-rules**
Adds, deletes, or replaces a firewall rule. **self-ip** rules are checked when a packet is received that is destined for a **self-ip** /port pair on which there is no **ltm virtual**.

- **action**
  Specifies the action that the system takes when a rule is matched.

- **accept**
  Specifies that the current packet should be accepted. The packet will be not be compared to any more firewall rules.
- **drop**
  Specifies that the current packet should be silently dropped. Nothing is sent back to the packet source. The packet is not compared to any other firewall rules.
- **reject**
  Specifies that the current packet should be dropped. For TCP based protocols, a TCP reset is sent to the source. For other protocols, **reject** is equivalent to **drop**.

- **description**
  User defined description.
- **destination**

  - **address-lists**
    Specifies a list of address lists against which the packet will be compared. See **security firewall address-list**.
  - **addresses**
    Specifies a list of addresses and networks against which the packet will be compared.
  - **port-lists**
    Specifies a list of port lists against which the packet will be compared. See **security firewall port-list**.
  - **ports**
    Specifies a list of ports and port ranges against which the packet will be compared.
- **icmp**
  Specifies a list of ICMP types and codes against which the packet will be compared. The standard integer identifiers are used to specify an ICMP type. Example: 3 is destination unreachable and 3:1 is destination unreachable with a code of host unreachable. The list of ICMP types and codes can be found at the following URL: http://www.iana.org/assignments/icmp-parameters/icmp-parameters.xml.
- **ip-protocol**
  Specifies the IP protocol against which the packet will be compared.
- **irule**
  Specifies the name of the iRule that will be triggered when a packet matches this firewall rule. The firewall rule match raises a FLOW_INIT iRule event.
- **irule-sample-rate**
  Specifies the rate at which an iRule specified by **irule** option will be triggered when a packet matches this firewall rule. The rate is an integer value in the range 0-65535 and specifies how many packets

must match this firewall rule before the iRule is triggered. The default value is 1 and causes the iRule to be triggered for every packet that matches this firewall rule. A value of 0 disables iRule triggering.

- **log**
  Specifies whether the packet will be logged if it matches the rule. Logging must also be enabled in the **security log profile global-network** configuration. Note that the statistics counter is always incremented when a packet matches a rule.
- **place-after**
  Specifies that a new rule should be placed after another rule, **first** or **last**. If individual rules are being added (as opposed to specifying **replace-all-with**), then **place-before** or **place-after** must be specified.
- **place-before**
  Specifies that a new rule should be placed before another rule, **first** or **last**. If individual rules are being added (as opposed to specifying **replace-all-with**), then **place-before** or **place-after** must be specified.
- **rule-list**
  Specifies a list of rules to evaluate. See **security firewall rule-list**. If a **rule-list** is specified, then only the **schedule** and **status** properties effect the rule.
- **schedule**
  Specifies a schedule for the rule. See **security firewall schedule**. If the rule refers to a **rule-list**, the **rule-list** will be enabled according to the schedule. When the **rule list** is enabled, the schedules defined within the **rule-list** will be honored.
- **source**

  - **address-lists**
    Specifies a list of address lists against which the packet will be compared. See **security firewall address-list**.
  - **addresses**
    Specifies a list of addresses and networks against which the packet will be compared.
  - **port-lists**
    Specifies a list of port lists against which the packet will be compared. See **security firewall port-list**.
  - **ports**
    Specifies a list of ports and port ranges against which the packet will be compared.
  - **vlans**
    Specifies a list of VLANs, VLAN groups and tunnels against which the packet will be compared.
- **status**
  Specifies whether the rule is **enabled**, **disabled** or **scheduled**. A rule that is **enabled** is always checked. A rule that is **disabled** is never

checked. A rule that is **scheduled** is checked according to the corresponding schedule configuration. A rule that is **scheduled** must have an associated schedule configuration.

- **fw-staged-policy**
  Specifies a staged firewall policy. **fw-staged-policy** rules are not enforced while all the visibility aspects namely statistics, reporting and logging function as if the **fw-staged-policy** rules were enforced on a self IP address.
- **fw-staged-policy-rules**
  Specifies firewall rules staged on **net self** via referenced **fw-staged-policy**.
- **glob**
  Displays the items that match the **glob** expression. See **help glob** for a description of **glob** expression syntax.
- **regex**
  Displays the items that match the regular expression. The regular expression must be preceded by an at sign (@[regular expression]) to indicate that the identifier is a regular expression. See **help regex** for a description of regular expression syntax.
- **unit**
  Read-only property that specifies the unit in a redundant system. Based on **traffic-group**.
- **traffic-group**
  Specifies the traffic group of the self IP address. The default traffic group is traffic-group-local-only, the non-floating traffic-group.
- **inherited-traffic-group**
  Read-only property that indicates if the **traffic-group** is inherited from the parent folder.
- **vlan**
  Specifies the VLAN for which you are setting a self IP address. This option is required.

See Also

create, *delete*, *edit*, glob, *list*, *modify*, *mv*, *self-allow*, *vlan*, *vlan-group*, regex, *profile*, *show*, *tmsh*

self-allow

Configures the default "allow list" for all self IP addresses on the BIG-IP® system when the option **allow-service** of the component **self** is set to **default**.

Syntax

Modify the **self-allow** component within the **net** module using the syntax shown in the following sections.

Modify

```
modify self-allow
   defaults [all | none]
   defaults
     [add | delete | replace-all-with] {
       [protocol:port] ...
   }
edit self-allow
  all-properties
```

Display

```
list self-allow
show running-config self-allow
   all-properties
   defaults
   one-line
```

Delete

```
You cannot delete the default allow list.
```

Description

You can use the **self-allow** component to modify or display the default allow list for all self IP addresses on the BIG-IP system when the option **allow-service** of the component **self** is set to **default**. The default allow list displays which service and protocol ports allow connections from outside the system. The system refuses connections made to a service or protocol port that is not on the list.

Examples

modify self-allow defaults all

Sets the default allow list to all. Then, if the value of the option **allow-service** of the **net self** component is **default**, the system accepts traffic from all protocol port combinations.

modify self-allow default replace-all-with { tcp:55 }

Sets the default "allow list" for all self IP addresses on the system to TCP on port 55.

list self-allow defaults

Displays the default "allow list" for all self IP addresses on the system.

Options

- **defaults**
  Specifies to set the default allow list to one of the following:
  - **all**
    Specifies that all protocols and services allow connections from outside the system. Use this option to open the system to complete access.
  - **none**
    Specifies that no protocols or services allow connections from outside the system.
  - **protocol:port**
    Specifies a list of protocols/services that allow connections from outside the system.
  - **replace-all-with**
    Specifies to replace the current protocols and services that allow connections from outside the system with the specified protocols and services.

See Also

edit, *list*, *modify*, *vlan*, *vlan-group*, *show*, *tmsh*

stp

Configures a Spanning Tree Protocol (STP) instance.

Syntax

Configure the **stp** component within the **net** module using the syntax shown in the following sections.

Create/Modify

```
create stp [all | [name] ]
modify stp [all | [name] ]
    app-service [[string] | none]
    description [string]
    instance-id [integer]
    interfaces [ add | delete | modify | replace-all-with ] {
      [interface name] {
        app-service [[string] | none]
        external-path-cost [integer]
        internal-path-cost [integer]
        priority [integer]
     }
    }
    interfaces none
    priority [integer]
    trunks [ add | delete | modify | replace-all-with ] {
      [interface name] {
        app-service [[string] | none]
        external-path-cost [integer]
        internal-path-cost [integer]
        priority [integer]
      }
    }
    trunks none
    vlans [ add | delete | replace-all-with ] {
      [vlan name ...]
    }
    vlans none
edit stp [ [ all | [name] | [glob] | [regex] ] ... ]
    all-properties
    non-default-properties
```

Display

```
list stp
list stp [ [ all | [name] | [glob] | [regex] ] ... ]
show stp running-config
show stp running-config [ [ all | [name] | [glob] | [regex] ] ... ]
    all-properties
    non-default-properties
    one-line
```

Delete

```
delete stp [all | [name] ]
```

Description

You can use the **stp** component to configure an STP instance.

Examples

list stp

Displays all STP instances on the system.

show running-config stp

Displays the running configuration information for all STP instances.

delete stp myStp2

Removes all members from the STP instance, and then deletes the instance itself.

Note that you cannot delete spanning tree instance **0** (the Common and Internal Spanning Tree). You can only use the command **delete** in Multiple Spanning Tree Protocol (MSTP) mode.

Options

- **app-service**
  Specifies the name of the application service to which the object belongs. The default value is **none**. **Note:** If the **strict-updates** option is **enabled** on the application service that owns the object, you cannot modify or delete the object. Only the application service can modify or delete the object.
- **description**
  User defined description.
- **external-path-cost**
  Specifies the external path cost number for either an interface or trunk. The default value is **20000**.
  Each network interface has an associated path cost within each spanning tree instance. The path cost represents the relative cost of sending network traffic through that interface. In calculating the spanning tree, the algorithm tries to minimize the total path cost between each point of the tree and the root bridge. By manipulating the path costs of different interfaces or trunks it is possible to steer traffic toward paths that are faster, more reliable, and/or more economical. Path costs can take values in the range **1** - **200,000,000**. The default path cost for an interface or a trunk is based on the maximum, not actual speed, of the interface or trunk.
  In MSTP mode there are two kinds of path cost: external and internal.

The external path cost applies only to spanning tree instance **0**, the Common and Internal Spanning Tree (CIST). It is used to calculate the cost to reach an adjacent spanning tree region.

- **glob**
  Displays the items that match the **glob** expression. See **help glob** for a description of **glob** expression syntax.
- **instance-id**
  The instance ID for this STP instance. In Multiple Spanning Tree Protocol (MSTP) mode, there will be exactly one STP instance with ID **0**. The instance ID can be a value between 1 and 255.
- **internal-path-cost**
  Specifies the internal path cost number for either an interface or trunk. The default value is **20000**.
  Each network interface has an associated path cost within each spanning tree instance. The path cost represents the relative cost of sending network traffic through that interface. In calculating the spanning tree, the algorithm tries to minimize the total path cost between each point of the tree and the root bridge. By manipulating the path costs of different interfaces or trunks it is possible to steer traffic toward paths that are faster, more reliable, and/or more economical. Path costs can take values in the range **1** - **200,000,000**. The default path cost for an interface or a trunk is based on the maximum, not actual speed, of the interface or trunk.
  In MSTP mode there are two kinds of path cost: external and internal. The internal path costs can be independently set for each spanning tree instance (including instance **0**) in MSTP mode. The internal path costs are used to calculate the costs of reaching adjacent bridges within the same spanning tree region.
- **priority**
  Specifies the priority number of either a bridge, interface, or trunk. The default value for a bridge is **61440**. The default value for both interfaces and trunks is **128**.
  Each bridge, interface, and trunk in a spanning tree instance has a priority value. The relative values of the priorities control the topology of the spanning tree chosen by the protocol. The bridge with the lowest priority value (numerically) will become the root of the spanning tree. Priority values vary from **0** - **61440** in steps of 4096.
- **regex**
  Displays the items that match the regular expression. The regular expression must be preceded by an at sign (@[regular expression]) to indicate that the identifier is a regular expression. See **help regex** for a description of regular expression syntax.
- **vlans**
  Specifies the VLANs that you want to add to, delete from, or replace-all-with for this STP instance.

See Also

create, *delete*, *edit*, glob, *list*, *modify*, *interface*, *trunk*, *vlan*, regex, *show*, *tmsh*

stp-globals

Configures spanning tree protocols on the system.

Syntax

Configure the **stp-globals** component within the **net** module using the syntax shown in the following sections.

Modify

```
modify stp-globals
    config-name [configuration name]
    config-revision [integer]
    description [string]
    fwd-delay [integer]
    hello-time [integer]
    max-age [integer]
    max-hops [integer]
    mode [disabled | mstp | passthru | rstp | stp]
    transmit-hold [integer]
edit stp-globals
    all-properties
    non-default-properties
```

Display

```
list stp-globals
show running-config stp-globals
    all-properties
    non-default-properties
    one-line
```

Description

Provides the ability to configure spanning tree protocols for the traffic management system. Spanning tree protocols are Layer 2 protocols for preventing bridging loops. The system supports multiple spanning tree protocol (MSTP), rapid spanning tree protocol (RSTP), and spanning tree protocol (STP).

Examples

modify stp-globals mode passthru

Sets the STP mode to **passthru**. Passthru mode forwards spanning tree bridge protocol data units (BPDUs) received on any interface to all other interfaces.

modify stp-globals mode disabled

Sets the STP mode to **disabled**. No MSTP, RSTP, or STP packets are transmitted or received on the interface or trunk, and the spanning tree algorithm exerts no control over forwarding or learning on the port or the trunk.

Options

- **config-name**
  Specifies the configuration name (1 - 32 characters in length) only when the spanning tree mode is MSTP. The default configuration name is a string representation of a globally unique MAC address belonging to the traffic management system.
  The MSTP standard introduces the concept of spanning tree regions, which are groups of adjacent bridges with identical configuration names, configuration revision levels, and assignments of VLANs to spanning tree instances.

◆ Note

The system default configuration name is a string representation of the globally unique MAC address of the traffic management system in which hyphens replace the colons in the standard MAC address. For example, the default configuration name 00-01-D7-68-11-80, represents the MAC address 00:01:D7:68:11:80.

- **config-revision**
  Specifies the revision level of the MSTP configuration only when the value of the **mode** option is **mstp**. The specified number must be in the range **0** through **65535**. The default value is **0** (zero).
- **description**
  User defined description.
- **fwd-delay**
  In the original STP, the forward delay parameter controlled the number of seconds for which an interface was blocked from forwarding network traffic after a reconfiguration of the spanning tree topology. This parameter has no effect when RSTP or MSTP are used, as long as all bridges in the spanning tree use the RSTP or MSTP protocol. If any legacy STP bridges are present, then neighboring bridges must fall back to the old protocol, whose reconfiguration time is affected by the value of the **fwd-delay** option. The default value is **15** seconds, and the valid range is **4** to **30**.
- **hello-time**
  Specifies the time interval in seconds between the periodic transmissions that communicate spanning tree information to the adjacent bridges in the network. The default value is **2** seconds, and the valid range is **1 - 10**. The default value is optimal in virtually all cases. F5 Networks recommends that you do not change the value of the **hello-time** option.

- **max-age**
  Specifies the number of seconds for which spanning tree information received from other bridges is considered valid. The default value is **20** seconds, and the valid range is **6** - **40** seconds.
- **max-hops**
  Specifies the maximum number of hops an MSTP packet can travel before it is discarded. Use this option only when the value of the **mode** option is **mstp**. The number of hops must be in the range of **1** to **255** hops. The default number of hops is **20**.
- **mode**
  Specifies one of three spanning tree modes:
  - **disabled**
    Specifies to discard spanning tree bridge protocol data units (BPDUs) received on any interface.
  - **mstp**
    Specifies multiple spanning tree protocol.
  - **passthru**
    Forwards spanning tree bridge protocol data units (BPDUs) received on any interface to all other interfaces. Essentially, passthru mode makes the traffic management system transparent to spanning tree BPDUs. This is the system default.
  - **rstp**
    Specifies rapid spanning tree protocol (RSTP) converges to a fully-connected state quickly.
  - **stp**
    The system supports STP mode for legacy systems. If STP is detected in the network, the traffic management system changes to STP mode even when the **mode** option is set to **disabled**, **mstp**, or **rstp**.
- **transmit hold**
  Specifies the absolute limit on the number of spanning tree protocol packets the traffic management system may transmit on a port in any **hello-time** interval. It is used to ensure that spanning tree packets do not unduly load the network even in unstable situations. The default value is **6** packets, and the valid range is **1** through **10** packets.

See Also

edit, *interface*, *list*, *modify*, *show*, *tmsh*

trunk

Configures a trunk with link aggregation.

Syntax

Modify the **trunk** component within the **net** module using the syntax shown in the following sections.

Create/Modify

```
create trunk [name]
modify trunk [name]
   app-service [[string] | none]
   bandwidth
   description [string]
   distribution-hash [dst-mac | src-dst-ipport | src-dst-mac]
   interfaces
     [add | delete | replace-all-with] {
       [name ... ]
   }
   lacp [disabled | enabled]
   lacp-mode [active | passive]
   lacp-timeout [short | long]
   link-select-policy [auto | maximum-bandwidth]
   mac-address [MAC address]
   stp [disabled | enabled]
   stp-reset
   qinq-ethertype [string]
edit trunk [ [ [name] | [glob] | [regex] ] ... ]
   all-properties
   non-default-properties
reset-stats trunk
reset-stats trunk [ [ [name] | [glob] | [regex] ] ... ]
```

Display

```
list trunk
list trunk [ [ [name] | [glob] | [regex] ] ... ]
show running-config trunk
show running-config trunk
  [ [ [name] | [glob] | [regex] ] ... ]
   all-properties
   cfg-mbr-count
   non-default-properties
   one-line
   working-mbr-count
show trunk
show trunk [ [ [name] | [glob] | [regex] ] ... ]
   all-properties
   (default | exa | gig | kil | meg | peta | raw | tera | yotta | zetta)
   detail
   field-fmt
```

Delete

```
delete trunk [all | [name]
```

Description

Link Aggregation allows multiple physical links to be treated as one logical link. It is also referred to as trunking.

The main objective of link aggregation is to provide increased bandwidth at a lower cost, without having to upgrade hardware. The bandwidth of the aggregated trunk is the sum of the capacity of individual member links. Thus, it provides an option for linearly incremental bandwidth as opposed to bandwidth options available through physical layer technology. The traffic management system supports link aggregation control protocol (LACP).

When a trunk is created, LACP is disabled by default. In this mode, no control packets are exchanged and the member links carry traffic as long as the physical layer is operational. In the event of physical link failure, an LACP member is removed from the aggregation.

Note that both endpoints of the trunk should have identical LACP configuration to work properly. A mixed configuration where one endpoint is LACP enabled and the other is LACP disabled, is not valid.

Examples

create trunk my_trunk interfaces add {1.1 1.2 1.3}

Creates a trunk named **my_trunk** that includes the interfaces **1.1**, **1.2**, and **1.3**.

modify trunk my_trunk lacp enabled

Enable LACP on the trunk named **my_trunk**.

modify trunk my_trunk lacp-mode active

Enable active LACP mode on the trunk **my_trunk**.

Options

- **app-service**
  Specifies the name of the application service to which the object belongs. The default value is **none**. **Note:** If the **strict-updates** option is **enabled** on the application service that owns the object, you cannot modify or delete the object. Only the application service can modify or delete the object.
- **bandwidth**
  Specifies the operation bandwidth in bytes per second.
- **cfg-mbr-count**
  Displays the number of configured members that are associated with this trunk.

- **description**
  User defined description.
- **distribution-hash**
  Specifies the basis for the hash that the system uses as the frame distribution algorithm. The system uses the resulting hash to determine which interface to use for forwarding traffic.
  When frames are transmitted on a trunk, they are distributed across the working member links. The distribution function ensures that the frames belonging to a particular conversation are neither mis-ordered nor duplicated at the receiving end. Distribution is done by calculating a hash value based on source and destination addresses carried in the frame and associating the hash value with a link. All frames with a particular hash value are transmitted on the same link, thereby maintaining frame order. The options are:
  - **dst-mac**
    Uses the destination MAC addresses to calculate the hash value.
  - **src-dst-mac**
    Uses the source, destination, and MAC addresses to calculate the hash value.
  - **src-dst-ipport**
    Uses the source and destination IP addresses and ports to calculate the hash value.
- **glob**
  Displays the items that match the **glob** expression. See **help glob** for a description of **glob** expression syntax.
- **id**
  Displays the ID of the trunk.
- **interfaces**
  Specifies the interfaces by name separated by spaces that you want to add to the trunk, delete from the trunk, or with which you want to replace all existing interfaces associated with the trunk.
- **lacp**
  Specifies, when enabled, that the system supports the link aggregation control protocol (LACP), which monitors the trunk by exchanging control packets over the member links to determine the health of the links. If LACP detects a failure in a member link, it removes the link from the link aggregation. LACP is **disabled** by default, for backward compatibility.
- **lacp-mode**
  Specifies the operation mode for LACP if the **lacp** option is **enabled** for the trunk. The options are:
  - **active**
    Specifies that the system periodically transmits LACP packets, regardless of the control value of the peer system.
  - **passive**
    Specifies that the system periodically transmits LACP packets, unless the control value of the peer system is **active**.

- **lacp-timeout**
  Specifies the rate at which the system sends the LACP control packets. The default value is **long**.
  The options are:
  - **long**
    Specifies that the system exchanges LACP packets every **30** seconds.
  - **short**
    Specifies that the system exchanges LACP packets every second.
- **link-select-policy**
  Sets the LACP policy that the trunk uses to determine which member link (interface) can handle new traffic.
  Link aggregation is allowed only when all the interfaces are operating at the same media speed and connected to the same partner aggregation system. When there is a mismatch among configured members due to configuration errors or topology changes (auto-negotiation), link selection policy determines which links become working members and form the aggregation.
  The options are:
  - **auto**
    Specifies that the system chooses the lowest numbered operational link as the reference link. All the members that have the same media speed and are connected to the same partner as that of the reference link are declared as working members, and they are aggregated. The other configured members do not carry traffic.
  - **maximum-bandwidth**
    Specifies that the system adds to the aggregation a subset of links that gives maximum aggregate bandwidth to the trunk.
- **mac-address**
  Specifies the media access control (MAC) address, which is associated with the trunk, in not case-sensitive hexadecimal colon notation, for example, **00:0b:09:88:00:9a**.
- **media**
  Displays the media settings for the trunk.
- **name**
  Specifies a unique name for the component. This option is required for the commands **create**, **delete**, and **modify**.
- **regex**
  Displays the items that match the regular expression. The regular expression must be preceded by an at sign (@[regular expression]) to indicate that the identifier is a regular expression. See **help regex** for a description of regular expression syntax.
- **stp**
  Enables or disables spanning tree protocols (STP). The default value is **enabled**.
  If you disable STP, the system does not transmit or receive STP, RSTP, or MSTP packets on the trunk, and STP has no control over forwarding or learning on the trunk.

- **stp-reset**
  Resets STP, which forces a migration check.
- **qinq-ethertype**
  Specifies the ether-type value used for the packets handled on this trunk when it is a member in a QinQ vlan. The ether-type can be set to **any string containing a valid hexadecimal 16 bits number**, or any of the well known ether-types: **0x8100**, **0x9100**, **0x88a8**. Default value is set to **0x8100**.
- **working-mbr-count**
  Displays the number of working members associated with this trunk.

See Also

create, *delete*, *edit*, glob, *list*, *modify*, *interface*, *vlan*, *vlan-group*, regex, *reset-stats*, *show*, *tmsh*

vlan

Configures a virtual local area network (VLAN).

Syntax

Modify the **vlan** component within the **net** module using the syntax shown in the following sections.

Create/Modify

```
create vlan [name]
modify vlan [name]
    app-service [[string] | none]
    auto-lasthop [default | enabled | disabled ]
    description [string]
    failsafe [disabled | enabled]
    failsafe-action [failover | failover-restart-tm | reboot | restart-all]
    failsafe-timeout [integer]
    interfaces
      [add | delete | modify | replace-all-with] {
        [name] ... {
          [tagged | untagged]
          tag-mode [ customer | service | double | none ]
        }
    }
    interfaces none
    learning [disable-drop | disable-forward | enable-forward]
    mtu [integer]
    sflow {
        poll-interval [integer]
        poll-interval-global [no | yes]
        sampling-rate [integer]
        sampling-rate-global [no | yes]
    }
    source-checking [disabled | enabled]
    tag [integer]
    customer-tag [[string] | none]
    cmp-hash [default | dst-ip | src-ip]
    dag-tunnel [outer | inner]
    dag-round-robin [disabled | enabled]
edit vlan [ [ [name] | [glob] | [regex] ] ... ]
    all-properties
    non-default-properties
```

Display

```
list vlan
list vlan [ [ [name] | [glob] | [regex] ] ... ]
show running-config vlan
show running-config vlan
  [ [ [name] | [glob] | [regex] ] ... ]
    all-properties
    non-default-properties
    one-line
```

```
show vlan
show vlan [ [ [name] | [glob] | [regex] ] ... ]
    all-properties
    (default | exa | gig | kil | meg | peta | raw | tera | yotta | zetta)
    field-fmt
```

Delete

```
delete vlan [name]
```

Description

VLANs are part of the configuration of the BIG-IP® network components. VLANs can be based on either ports or tags. When creating a VLAN, a tag value for the VLAN is automatically chosen unless you specify a tag value on the command line.

VLANs can have both tagged and untagged interfaces. You can add an interface to multiple VLANs as a tagged interface. You can add an interface to a single VLAN as an untagged interface. The tagged traffic can be single tagged and double tagged.

◆ Note

*To reset the statistics that display when you use the command sequence **show vlan**, you must reset the statistics for the trunks and interfaces associated with the VLAN.*

Examples

create vlan my_vlan interfaces add { 1.2 1.3 1.4 }

Create the VLAN **my_vlan** that includes the interfaces **1.2**, **1.3**, and **1.4**.

delete vlan my_vlan

Delete the VLAN named **my_vlan**.

Options

- **app-service**
  Specifies the name of the application service to which the object belongs. The default value is **none**. **Note:** If the **strict-updates** option is **enabled** on the application service that owns the object, you cannot modify or delete the object. Only the application service can modify or delete the object.
- **description**
  User-defined description.
- **failsafe**
  Enables a fail-safe mechanism that causes the active cluster to fail over to a redundant cluster when loss of traffic is detected on a VLAN, and

traffic is not restored during the failover timeout period for that VLAN. The default value is **disabled**.
When you set the VLAN failsafe option to **enabled**, the default failsafe-action value is **restart-all**. Therefore, when the fail-safe mechanism is triggered, all the daemons are restarted and the unit fails over.

- **failsafe-action**
  Specifies the action for the system to take when the fail-safe mechanism is triggered. The default value is **failover-restart-tm**.
- **failsafe-timeout**
  Specifies the number of seconds that an active unit can run without detecting network traffic on this VLAN before it starts a failover. The default value is **90** seconds.
- **glob**
  Displays the items that match the **glob** expression. See **help glob** for a description of **glob** expression syntax.
- **if-index**
  Displays the index assigned to this VLAN. It is a unique identifier assigned for all objects displayed in the SNMP IF-MIB.
- **interfaces**
  Specifies a list of tagged or untagged interfaces and trunks that you want to configure for the VLAN. Use tagged interfaces or trunks when you want to assign a single interface or trunk to multiple VLANs.
  A tagged interface is one that you assign to a VLAN in a way that causes the system to add a VLAN tag into the header of any frame passing through that interface or trunk.
  A trunk is a combination of two or more interfaces and cables configured as one link.
  - **tag-mode**
    Specifies the tag mode of the interface or trunk associated with. The default value is **none**.
    The available values are:
    - **customer**
      Specifies tag-mode setting for vlan members that are facing customer network and carry single tagged traffic.
    - **service**
      Specifies tag-mode setting for vlan members that are facing the service provider networks and carry single tagged traffic.
    - **double**
      Specifies tag-mode setting for vlan members that are facing the service provider networks and carry double tagged traffic.
    - **none**
      Specifies no tag-mode setting.
  - **learning**
    Specifies whether switch ports placed in the VLAN are configured for switch learning, forwarding only, or dropped. The default value is **enable-forward**.

- **mtu**
  Sets a specific maximum transition unit (MTU) for the VLAN. The default value is **1500**. This value does not include the layer2 header.
- **name**
  Specifies a unique name for the component. This option is required for the commands **create**, **delete**, and **modify**.
- **regex**
  Displays the items that match the regular expression. The regular expression must be preceded by an at sign (@[regular expression]) to indicate that the identifier is a regular expression. See **help regex** for a description of regular expression syntax.
- **sflow**
  Specifies sFlow settings for the VLAN:
  - **poll-interval**
    Specifies the maximum interval in seconds between two pollings. The default value is **0**. To enable this setting, you must also set the **poll-interval-global** setting to **no**.
  - **poll-interval-global**
    Specifies whether the global VLAN poll-interval setting, which is available under **sys sflow global-settings** module, overrides the object-level poll-interval setting. The default value is **yes**.
    The available values are:
  - **no**
    Specifies to use the object-level poll-interval setting.
  - **yes**
    Specifies to use the global VLAN poll-interval setting.
  - **sampling-rate**
    Specifies the ratio of packets observed to the samples generated. For example, a sampling rate of 2000 specifies that 1 sample will be randomly generated for every 2000 packets observed. The default value is **0**. To enable this setting, you must also set the **sampling-rate-global** setting to **no**.
  - **sampling-rate-global**
    Specifies whether the global VLAN sampling-rate setting, which is available under **sys sflow global-settings** module, overrides the object-level sampling-rate setting. The default value is **yes**.
    The available values are:
  - **no**
    Specifies to use the object-level sampling-rate setting.
  - **yes**
    Specifies to use the global VLAN sampling-rate setting.
- **source-checking**
  Specifies that only connections that have a return route in the routing table are accepted. The default value is **disabled**.

- **tag**
  Specifies a number that the system adds into the header of any frame passing through the VLAN. The value can be **1** through **4094**. The default is to not use this option, and the system assigns a tag number.
- **customer-tag**
  Specifies a number that the system adds into the header of any double tagged frame passing through the VLAN. The value can be any of the following: **1** through **4094**, or **none**. The default is **none**.
- **cmp-hash**
  Specifies how the traffic on the VLAN will be disaggregated. The traffic disaggregation on the VLAN can be based on source ip, dest ip, or L4 ports. The default cmp hash uses L4 ports.
- **dag-tunnel**
  Specifies whether the ip tunnel traffic on the VLAN should be disaggregated based on the inner ip header or outer ip header.
- **dag-round-robin**
  Specifies whether some of the stateless traffic on the VLAN should be disaggregated in a round-robin order instead of using static hash. The stateless traffic include nonIP L2 traffic, ICMP, some UDP protocols, etc.

See Also

create, *delete*, *edit*, glob, *list*, *virtual*, *modify*, *interface*, *self*, *vlan-group*, regex, *show*, *tmsh*

vlan-allowed

Displays a list of available VLANs which can be used by the system.

Syntax

Display the **vlan-allowed** component within the **net** module using the syntax shown in the following sections.

Display

```
show vlan-allowed
    field-fmt
```

Description

Displays a list of available VLANs which can be used by the system.

See Also

show, *tmsh*

vlan-group

Configures a VLAN group.

Syntax

Modify the **vlan-group** component within the **net** module using the syntax shown in the following sections.

Create/Modify

```
create vlan-group [name]
modify vlan-group [name]
    app-service [[string] | none]
    auto-lasthop [default | enabled | disabled ]
    bridge-in-standby [disabled | enabled]
    bridge-multicast [disabled | enabled]
    bridge-traffic [disabled | enabled]
    description [string]
    members
      [add | delete | replace-all-with] ] {
        [vlan name] ...
    }
    members [default | none]
    migration-keepalive [disabled | enabled]
    mode [opaque | translucent | transparent]
    proxy-excludes
      [add | delete | replace-all-with] ] {
        [ip address] ...
    }
    proxy-excludes [default | none]
    tag [integer]
edit vlan-group [ [ [name] | [glob] | [regex] ] ... ]
    all-properties
    non-default-properties
```

Display

```
list vlan-group
list vlan-group [ [ [name] | [glob] | [regex] ] ... ]
show running-config vlan-group
show running-config vlan-group
  [ [ [name] | [glob] | [regex] ] ... ]
    all-properties
    non-default-properties
    one-line
show vlan-group
show vlan-group [ [ [name] | [glob] | [regex] ] ... ]
    all-properties
    (default | exa | gig | kil | meg | peta | raw | tera | yotta | zetta)
    field-fmt
```

Delete

```
delete vlan-group [name]
```

Description

The **vlan-group** component defines a VLAN group, which is a grouping of two or more VLANs belonging to the same IP network for the purpose of allowing Layer 2 packet forwarding between those VLANs.

The VLANs between which the packets are to be passed must be on the same IP network, and they must be grouped using the vlan-group component. For example: **modify vlan-group network11 members add { internal external }**.

Examples

create vlan-group my_vlan-group members add { vlan1 vlan2 }

Creates a VLAN group named **my_vlan-group** that consists of VLANs named **vlan1** and **vlan2**.

modify vlan-group proxy-excludes add { 10.10.10.1 }

Sets the global VLAN group proxy exclusion list.

delete vlan-group my_vlan-group

Deletes the VLAN group named **my_vlan-group**.

Options

- **app-service**
  Specifies the name of the application service to which the object belongs. The default value is **none**. **Note:** If the **strict-updates** option is **enabled** on the application service that owns the object, you cannot modify or delete the object. Only the application service can modify or delete the object.
- **bridge-traffic**
  When enabled, specifies that the VLAN group forwards all frames, including non-IP traffic. The default value is **disabled**.
- **bridge-in-standby**
  When enabled, specifies that the VLAN group forwards packets, even when the system is the standby unit in a redundant system. This option is designed for deployments in which the VLAN group exists on only one of the units. If that does not match your configuration, using this option may cause adverse effects. The default value is **enabled**.
- **bridge-multicast**
  When enabled, allows bridging of non-Internet Protocol (IP) Address Resolution Protocol (ARP) multicast frames across a VLAN group. An example of when you might want to use this option is when you are implementing the Spanning Tree Protocol (STP).
- **description**
  User-defined description.

- **glob**
  Displays the items that match the **glob** expression. See **help glob** for a description of **glob** expression syntax.
- **members**
  The names of the VLANs that you want to add to or delete from the VLAN group.
- **migration-keepalive**
  Specifies whether the system will send keepalive frames (TCP keepalives and empty UDP packets depending on the connection type) when a node is moved from one VLAN group member to another VLAN group member for all existing connections that the system has to that node.
- **mode**
  Specifies the level of exposure of remote MAC addresses within VLAN groups. The default value is **translucent**.
  The options are:
  - **opaque**
    Use this option when you have a Cisco router in the network sending CDP packets to the system. Because opaque VLAN groups require a source and destination MAC address, and CDP packets do not contain a source and destination MAC address, the CDP packets are not forwarded through the VLAN group. This mode changes the MAC address to the MAC address assigned to the VLAN group, a proxy ARP with Layer 3 forwarding.
  - **translucent**
    Uses the real MAC address of the requested host with the locally unique bit toggled. Specifies that the system uses Layer 2 forwarding with locally-unique bit, toggled in ARP response across VLANs.
  - **transparent**
    Leaves the MAC address unchanged by the traffic management system. Specifies that the system uses Layer 2 forwarding with the original MAC address of the remote system preserved across VLANs.
- **name**
  Specifies a unique name for the component. This option is required for the commands **create**, **delete**, and **modify**.
- **proxy-excludes**
  Specifies the IP addresses that you want to include in the proxy ARP exclusion list. If you use VLAN groups, you must configure a proxy ARP forwarding exclusion list. F5 Networks recommends that you configure this feature if you use VLAN groups with a redundant system. The reason is that both units need to communicate directly with their gateways and the back-end nodes. Creating a proxy ARP exclusion list prevents traffic from being proxied through the active unit due to proxy ARP. This traffic needs to be sent directly to the destination, not proxied.
- **regex**
  Displays the items that match the regular expression. The regular expression must be preceded by an at sign (@[regular expression]) to indicate that the identifier is a regular expression. See **help regex** for a description of regular expression syntax.

- **tag**
  Specifies a number from **1** through **4094** to be the tag for the VLAN. A VLAN tag is an identification number the system inserts into the header of a frame that indicates the VLAN to which the destination device belongs. Use VLAN tags when a single interface forwards traffic for multiple VLANs.

See Also

create, *delete*, *edit*, glob, *list*, *modify*, *interface*, *self*, *vlan*, regex, *show*, *tmsh*

wccp

Configures Web Cache Communication Protocol (WCCP) services.

Syntax

Configure the **wccp** component within the **net** module using the syntax in the following sections.

Create/Modify

```
create wccp [name]
modify wccp [name]
    app-service [[string] | none]
    cache-timeout [integer]
    description [string]
    services [add | delete | replace-all-with] {
      [object identifier] {
          app-service [[string] | none]
          hash-fields [dest-ip | dest-port | src-ip | src-port | none]
          password [string | none]
          port-type [none | dest | source]
          ports [integer]
          priority [integer]
          protocol [tcp | udp]
          redirection-method [gre | l2]
          return-method [gre | l2]
          routers [add | delete | replace-all-with] {
            [ip address ...]
          }
          traffic-assign [hash | mask]
          tunnel-local-address [ip address]
          tunnel-remote-addresses [add | delete | replace-all-with] {
            [ip address ...]
          }
          weight [integer]
       }
    }
edit wccp [ [ [name] | [glob] | [regex] ] ... ]
    all-properties
    non-default-properties
```

Display

```
list wccp
list wccp [ [ [name] | [glob] | [regex] ] ... ]
show running-config wccp
show running-config wccp [ [ [name] | [glob] | [regex] ] ... ]
    all-properties
    non-default-properties
    one-line
```

Delete

```
delete wccp [name]
```

Description

You can use the **wccp** component to create and modify WCCPv2 service groups. WCCPv2 is a content-routing protocol developed by Cisco Systems, Inc., which provides a mechanism to redirect traffic flows in real time. A WCCP service in this context is a set of redirection criteria and processing instructions that the BIG-IP® system applies to any traffic that a router in the service group redirects to the BIG-IP system.

Examples

list wccp service-wccp all-properties

Displays the services and their attributes in the service group named **service-wccp**.

modify server-wccp cache-timeout 40

Changes the cache-timeout setting to **40** for the service group named **server-wccp**.

modify server-wccp services modify { 77 {weight 60} }

Changes the weight setting to **60** for the service identified as **77** in the service group named **server-wccp**.

Options

- **app-service**
  Specifies the name of the application service to which the object belongs. The default value is **none**. **Note:** If the **strict-updates** option is **enabled** on the application service that owns the object, you cannot modify or delete the object. Only the application service can modify or delete the object.
- **cache-timeout**
  Specifies the frequency of control messages between the system and the router. The range is from **1** to **60** seconds. The default value is **10**.
- **description**
  User-defined description.
- **glob**
  Displays the items that match the **glob** expression. See **help glob** for a description of **glob** expression syntax.
- **name**
  Specifies a unique name for the component. This option is required for the commands **create**, **delete**, and **modify**.
- **regex**
  Displays the items that match the regular expression. The regular expression must be preceded by an at sign (@[regular expression]) to indicate that the identifier is a regular expression. See **help regex** for a description of regular expression syntax.

- **services**
  Specifies the service group identifier, a number between **51** and **255** that matches a service ID configured on the router.
  Adds, deletes, or replaces a set of services. You can configure the following options for a service:
  - **app-service**
    Specifies the name of the application service to which the service belongs. The default value is **none**. **Note:** If the **strict-updates** option is **enabled** on the application service that owns the object, you cannot modify or delete the service. Only the application service can modify or delete the service.
  - **hash-fields**
    Specifies to the router which traffic attributes to use to determine which BIG-IP system it should forward traffic to for load balancing: destination IP address (**dest-ip**), destination port (**dest-port**), source IP address (**src-ip**), and/or source port (**src-port**).
  - **object identifier**
    Specifies the service group identifier, a number between **51** and **255** that matches a service ID configured on the router.
  - **password**
    Specifies the password for MD5 authentication or **none**.
  - **port-type**
    Specifies whether the WCCP interception of traffic is based on the destination port (**dest**) or source port (**source**), or is not specified (**none**). The default value is **none**.
  - **ports**
    Specifies one or more ports (up to 8) on which traffic is redirected.
  - **priority**
    Specifies the precedence of the service group relative to the other service groups. The range is from **1** to **255**. The default value is **100**.
  - **protocol**
    Specifies the protocol of the traffic to be redirected: TCP (**tcp**) or UDP (**udp**). The default value is **tcp**.
  - **redirection**
    Specifies the method the router uses to redirect traffic: GRE **gre** or L2 **l2**. The default value is **gre**.
  - **return**
    Specifies the method used to return passthrough traffic to the router: GRE (**gre**) or L2 (**l2**). The default value is **gre**.
  - **routers**
    Specifies the IP addresses of the WCCP-enabled routers that redirect traffic.
  - **traffic-assign**
    Specifies whether load balancing is achieved by a hash algorithm or a mask. If you specify **hash**, specify one or more attributes using the option **hash-fields**.

- **tunnel-local-address**
  Specifies an IP address on the BIG-IP system to which the WCCP-enabled routers should redirect traffic. Specify a self IP address of an external VLAN on the BIG-IP system.
- **tunnel-remote-addresses**
  Specifies the Router Identifier IP address of the router that redirects traffic.
- **weight**
  Specifies the relative importance of this traffic in a load-balancing environment. The range is from **1** to **100**. The default value is **50**.

See Also

create, *delete*, *edit*, glob, *list*, *modify*, regex, *show*, *tmsh*

69

net cos

- Introducing the net cos module
- Alphabetical list of components

Introducing the net cos module

You can use the tmsh components that reside within the Network Class of Service (net cos) module to manipulate the Class of Service fields in Ethernet frames. The CoS field is useful for various data and voice protocols.

For more information about the tmsh hierarchical structure, see Chapter 2, *Understanding and Using the Traffic Management Shell*.

Alphabetical list of components

The remainder of this chapter lists the tmsh components that are available in the net cos module.

global-settings

Configures the global configuration for class of service (CoS).

Syntax

Modify the **global-settings** component within the **net cos** module using the syntax shown in the following sections.

Create/Modify

```
modify global-settings
    feature-enabled
    feature-disabled
    precedence [dscp-only, 8021p-only]
    default-map-dscp
      [add | delete | modify | replace-all-with] {
          [map-dscp-name] ...
    }
    default-map-8021p
      [add | delete | modify | replace-all-with] {
          [map-8021p-name] ...
    }
    default-traffic-priority [ traffic-priority-name ]
```

Display

```
list global-settings
    all-properties
    non-default-properties
    one-line
show global-settings
```

Description

You can use the global-settings component to configure and view information about the global settings of all CoS behavior.

show keyword displays an analysis of the relative weights of the associated traffic-priority objects.

Examples

modify global-settings default-traffic-priority NORMAL_PRIORITY

Replace the default traffic-priority with traffic-priority **NORMAL_PRIORITY**.

modify global-settings default-map-8021p add { VOIP }

Add the VOIP 802.1p mapping. The VOIP object specifies the 802.1p field value and associated traffic priority.

Options

- **feature-enabled**
  Enable 8 hardware egress CoS queue feature.
- **feature-disabled**
  Disable 8 hardware egress CoS queue feature.
- **precedence**
  Specifies the precedence between handling of DSCP and 802.1p. Currently, provided options are **dscp-only** and **8021p-only**.
- **default-map-dscp**
  Enables adding and removal of mappings between DSCP field values and traffic priorities. See **net cos traffic-priority** and **net cos map-dscp**.
- **default-map-8021p**
  Enables adding and removal of mappings between 802.1p field values and traffic priorities.
- **default-traffic-priority**
  Specifies the default **traffic-priority** which is applied to all traffic that does not match a specified DSCP/802.1p field value. This allows the user to specify only the mappings which do not match the default.

See Also

traffic-priority, *map-dscp*

map-8021p

Configures vlan 8021.p tag to traffic priority mapping.

Syntax

Modify the **map-8021p** component within the **net cos** module using the syntax shown in the following sections.

Create/Modify

```
create map-8021p [name]
modify map-8021p [name]
    value [0..7]
    traffic-priority [name]
edit map-8021p [ [ [name] | [glob] | [regex] ] ... ]
    all-properties
    non-default-properties
```

Display

```
list map-8021p
list map-8021p [ [ [name] | [glob] | [regex] ] ... ]
show map-8021p
show map-8021p [ [ [name] | [glob] | [regex] ] ... ]
    all-properties
    (default | exa | gig | kil | meg | peta | raw | tera | yotta | zetta)
    field-fmt
```

Delete

```
delete map-8021p [name]
```

Description

The **map-8021p** object allows users to associate 802.1p field values to relative traffic priority. These objects are associated with active system configuration via **net cos global-settings**.

Examples

create map-8021p VOIP value 4 traffic-priority HIGH_PRIORITY

Create the **map-8021p** named VOIP that associates 802.1p value 4 traffic with **traffic-priority** named HIGH_PRIORITY.

delete map-8021p VOIP

Delete the **map-8021p** named VOIP.

Options

- **value**
  Specifies the 802.1p field value.
- **traffic-priority**
  Specifies the **traffic-priority** object associated with traffic matching value.

See Also

create, *delete*, *edit*, glob, *list*, *global-settings*, *modify*, *traffic-priority*, *map-dscp*, regex, *show*, *tmsh*

map-dscp

Configures IP DSCP field to traffic priority mapping.

Syntax

Modify the **map-dscp** component within the **net cos** module using the syntax shown in the following sections.

Create/Modify

```
create map-dscp [name]
modify map-dscp [name]
    value [0..7]
    traffic-priority [name]
edit map-dscp [ [ [name] | [glob] | [regex] ] ... ]
    all-properties
    non-default-properties
```

Display

```
list map-dscp
list map-dscp [ [ [name] | [glob] | [regex] ] ... ]
show map-dscp
show map-dscp [ [ [name] | [glob] | [regex] ] ... ]
    all-properties
    (default | exa | gig | kil | meg | peta | raw | tera | yotta | zetta)
    field-fmt
```

Delete

```
delete map-dscp [name]
```

Description

The **map-dscp** object allows users to associate DSCP field values to relative traffic priority. These objects are associated with active system configuration via **net cos global-settings**.

Examples

create map-dscp VOIP value 4 traffic-priority HIGH_PRIORITY

Create the **map-dscp** named VOIP that associates DSCP value 4 traffic with **traffic-priority** named HIGH_PRIORITY.

delete map-dscp VOIP

Delete the **map-dscp** named VOIP.

Options

- **value**
  Specifies the DSCP field value.
- **traffic-priority**
  Specifies the **traffic-priority** object associated with traffic matching value.

See Also

create, *delete*, *edit*, glob, *list*, *global-settings*, *modify*, *traffic-priority*, *map-dscp*, regex, *show*, *tmsh*

traffic-priority

Configures a traffic priority object.

Syntax

Modify the **traffic-priority** component within the **net cos** module using the syntax shown in the following sections.

Create/Modify

```
create traffic-priority [name]
modify traffic-priority [name]
    weight [1..127]
    buffer [1..127]
edit traffic-priority [ [ [name] | [glob] | [regex] ] ... ]
    all-properties
    non-default-properties
```

Display

```
list traffic-priority
list traffic-priority [ [ [name] | [glob] | [regex] ] ... ]
show traffic-priority
show traffic-priority [ [ [name] | [glob] | [regex] ] ... ]
    all-properties
    (default | exa | gig | kil | meg | peta | raw | tera | yotta | zetta)
    field-fmt
```

Delete

```
delete traffic-priority [name]
```

Description

The **traffic-priority** object allows users to assign relative scheduling and buffer weightings. These objects are associated to specific traffic with **net cos map-dscp** and **net cos map-8021p**. There can be at most 8 traffic-priorities defined in the system. The **DEFAULT_PRIORITY** priority may be deleted or modifed as desired.

Examples

create traffic-priority HIGH_PRIORITY weight 127

Create the **traffic-priority** HIGH_PRIORITY that has a weight of 127.

delete traffic-priority HIGH_PRIORITY

Delete the **traffic-priority** named HIGH_PRIORITY.

Options

- **weight**
  Specifies the egress buffer weight. This value is used relative to other egress **traffic-priority** objects typical of weighted round-robin behavior.
- **buffer**
  Specifies the relative buffer weight where available egress buffer space is distributed with consistent relative weight.

See Also

create, *delete*, *edit*, glob, *list*, *global-settings*, *modify*, *map-dscp*, *map-8021p*, regex, *show*, *tmsh*

70

net dns-resolver

- Introducing the net dns-resolver module
- Alphabetical list of components

Introducing the net dns-resolver module

You can use the tmsh components that reside within the net dns-resolver module to configure a DNS resolver on this BIG-IP system. For more information about the tmsh hierarchical structure, see Chapter 2, *Understanding and Using the Traffic Management Shell*.

Alphabetical list of components

The remainder of this chapter lists the tmsh components that are available in the net dns-resolver module.

resolver

Configures a DNS resolver on the BIG-IP® system.

Syntax

Configure the DNS **resolver** component using the syntax in the following sections.

Create/Modify

```
create [name]
modify [name]
    answer-default-zones [yes | no]
    cache-size [integer]
    forward-zones [add | delete | modify | replace-all-with] {
      [ [zone-name] ] {
          nameservers [add | delete | replace-all-with] {
            [ [IPv4address:port] | [IPv6address.port] ]
          }
          nameservers none
    }
    forward-zones none
    randomize-query-name-case [yes | no]
    route-domain [name]
    use-ipv4 [yes | no]
    use-ipv6 [yes | no]
    use-tcp [yes | no]
    use-udp [yes | no]
```

Display

```
list
list [ [ [name] | [glob] | [regex] ] ... ]
    all-properties
    non-default-properties
    one-line
show [name]
reset-stats
```

Delete

```
delete resolver [name]
```

Description

You can use the **dns-resolver** component to configure and view information about a DNS Resolver object. A DNS resolver performs recursive resolution to fill its cache.

Important

When sizing caches, consider the total amount of memory available and how you wish to allocate memory for DNS caching. Note that cache sizing values are per-TMM process; therefore, a platform with eight TMMs consumes the amount of memory set for the Resolver object times eight.

Important

DNS Resolver objects use the DNS root nameservers published by InterNIC.

Examples

list

Displays the properties of the DNS Resolver **myRes**.

Options

- **answer-default-zones**
  Specifies whether the resolver answers queries for default zones: localhost, reverse 127.0.0.1 and ::1, and AS112 zones. The default value is **no**.
- **cache-size**
  Specifies the maximum cache size in bytes of the DNS Resolver object. The default value is **5767168**.
  The BIG-IP system caches the supporting records in a DNS response in the resource record cache. After the maximum size of the cache is reached, when new or refreshed content is added to the cache, the expired and older content is removed from the cache. A higher maximum size allows more DNS responses to be cached and increases the cache hit percentage. A lower maximum size forces earlier eviction of cached content, but can lower the cache hit percentage.
- **forward-zones**
  Adds, deletes, modifies, or replaces a set of forward zones on a DNS Resolver, by specifying zone name(s). A given zone name should only use the symbols allowed for a fully qualified domain name (FQDN), namely ASCII letters **a** though **z**, digits **0** through **9**, hyphen **-**, and period **.**. For example **site.example.com** would be a valid zone name.
  A DNS Resolver configured with a forward zone will forward any queries that resulted in a cache-miss (the answer was not available in the cache) and which also match a configured zone name, to the nameserver specified on the zone. If no nameservers are specified on the zone, an

automatic SERVFAIL is returned. When a forward zone's nameserver returns a valid response to the DNS Cache, that response is cached and then returned to the requestor.

- **nameservers**
  Adds, deletes, modifies, or replaces a set of nameservers in a forward zone on a DNS Resolver. A nameserver is represented by an **IPaddress** and **port** in the format **[IPv4:port]** or **[IPv6.port]**, for example **10.10.10.10:53** or **2001::1:ff.53**, respectively.
  If more than one nameserver is listed for a given forward zone, a matching query will be sent to the nameserver that is currently deemed the most responsive (based on RTTs). If no response is received within a certain window of time, the DNS Resolver will resend the query to another nameserver with an increased wait window, until a response is received.

- **glob**
  Displays the items that match the **glob** expression. See **help glob** for a description of **glob** expression syntax.
- **name**
  Specifies a unique name for the component. This option is required for the commands **create**, **delete**, and **modify**.
- **randomize-query-name-case**
  Specifies whether the resolver randomizes the case of query names. The default value is **yes**.
- **regex**
  Displays the items that match the regular expression. The regular expression must be preceded by an at sign (@[regular expression]) to indicate that the identifier is a regular expression. See **help regex** for a description of regular expression syntax.
- **route-domain**
  Specifies the route domain the resolver uses for outbound traffic. The default value is the default route domain.
- **use-ipv4**
  Specifies whether the resolver sends DNS queries to IPv4 addresses. The default value is **yes**.
- **use-ipv6**
  Specifies whether the resolver sends DNS queries to IPv6 addresses. The default value is **yes**.
- **use-tcp**
  Specifies whether the resolver can send queries over the TCP protocol. The default value is **yes**.
- **use-udp**
  Specifies whether the resolver can send queries over the UDP protocol. The default value is **yes**.

See Also

create, *delete*, *edit*, glob, *list*, *show*, *modify*, regex, *tmsh*

71

net fdb

- Introducing the net fdb module
- Alphabetical list of components

Introducing the net fdb module

You can use the tmsh components that reside within the net fdb module to configure the network. For more information about the tmsh hierarchical structure, see Chapter 2, *Understanding and Using the Traffic Management Shell*.

Alphabetical list of components

The remainder of this chapter lists the tmsh components that are available in the net module.

tunnel

Manages tunnel entries in the Layer 2 Forwarding table.

Syntax

Configure the **tunnel** component within the **net fdb** module using the syntax in the following sections.

Display

```
show tunnel
show tunnel [ [ [tunnel name] | [glob] | [regex] ] ... ]
    dynamic
    field-fmt
```

Description

You can use the **tunnel** component to manage tunnel entries in the Layer 2 Forwarding tables.

Examples

show tunnel

Displays all dynamic tunnel entries in the Layer 2 Forwarding table.

Options

- **all-records**
  Shows, from the specified Tunnel, all dynamic records.
- **dynamic**
  Displays all dynamic tunnel entries in the Layer 2 Forwarding table.
- **glob**
  Displays the items that match the **glob** expression. See **help glob** for a description of **glob** expression syntax.
- **regex**
  Displays the items that match the regular expression. The regular expression must be preceded by an at sign (@[regular expression]) to indicate that the identifier is a regular expression. See **help regex** for a description of regular expression syntax.

See Also

glob, *net tunnels*, regex, *show*, *tmsh*

vlan

Manages VLAN entries in the Layer 2 Forwarding table.

Syntax

Configure the **vlan** component within the **net fdb** module using the syntax in the following sections.

Modify

```
modify vlan [vlan name]
    app-service [[string] | none]
    records
      [add | delete | modify | replace-all-with] {
        [MAC address] ... {
          app-service [[string] | none]
          description [string]
          trunk [trunk name]
          interface [interface name]
        }
    }
    records none
edit vlan [ [ all | [vlan name] | [glob] | [regex] ] ... ]
    all-properties
    non-default-properties
```

Display

```
list vlan
list vlan [ [ [vlan name] | [glob] | [regex] ] ... ]
show running-config vlan
show running-config vlan [ [vlan name] | [glob] | [regex] ] ... ]
    all-properties
    non-default-properties
    one-line
    partition
    records
show vlan
show vlan [ [ [vlan name] | [glob] | [regex] ] ... ]
    dynamic
    field-fmt
    static
```

Delete

```
delete vlan
delete vlan [all | [vlan name] ]
    all-records
    dynamic
    static
```

Description

You can use the **vlan** component to manage entries in VLAN Layer 2 Forwarding tables.

Examples

modify vlan internal records add { 00:0b:09:88:00:9a { interface 1.2 } }

Creates a mapping of the MAC address 00:0b:09:88:00:9a to interface 1.2 on VLAN internal.

modify vlan internal records modify { 00:0b:09:88:00:9a { interface 1.1 } }

Modifies the mapping of the MAC address 00:0b:09:88:00:9a to interface 1.1 on VLAN internal.

show vlan

Displays all dynamic and static entries in the Layer 2 Forwarding table.

list vlan all-properties

Displays all properties for all static entries in the Layer 2 Forwarding table.

list vlan non-default-properties

Displays all non-default properties for all static entries in the Layer 2 Forwarding table.

delete vlan all

Deletes all entries in all VLAN Layer 2 Forwarding tables.

Options

- **app-service**
  Specifies the name of the application service to which the object belongs. The default value is **none**. **Note:** If the **strict-updates** option is **enabled** on the application service that owns the object, you cannot modify or delete the object. Only the application service can modify or delete the object.
- **all-records**
  Deletes, from the specified VLAN, all dynamic and static records.
- **description**
  User defined description.
- **dynamic**
  Displays or deletes all dynamic entries in the Layer 2 Forwarding table.
- **glob**
  Displays the items that match the **glob** expression. See **help glob** for a description of **glob** expression syntax.

- **interface**
  Specifies an interface to which you want to map a MAC address. You must specify either an interface or a trunk when you create an entry in the Layer 2 Forwarding table.
- **MAC address**
  Specifies a 6-byte ethernet address in not case-sensitive hexadecimal colon notation, for example, **00:0b:09:88:00:9a**. You must specify a MAC address when you create an entry in the Layer 2 Forwarding table.
- **partition**
  Displays the administrative partition in which the VLAN resides.
- **records**
  Specifies MAC addresses for the VLAN Layer 2 Forwarding table. Specifies MAC addresses that you want to add to, delete from, modify, or replace in the VLAN Layer 2 Forwarding table.
- **regex**
  Displays the items that match the regular expression. The regular expression must be preceded by an at sign (@[regular expression]) to indicate that the identifier is a regular expression. See **help regex** for a description of regular expression syntax.
- **static**
  Displays or deletes all static entries in the Layer 2 Forwarding table.
- **trunk**
  Specifies a trunk to which you want to map a MAC address. You must specify either an interface or a trunk when you create an entry in the Layer 2 Forwarding table.

See Also

delete, *edit*, glob, *list*, *modify*, *vlan*, regex, *show*, *tmsh*

72

net ipsec

- Introducing the net ipsec module
- Alphabetical list of components

Introducing the net ipsec module

You can use the tmsh components that reside within the net ipsec module to configure IP security for the BIG-IP® system. For more information about the tmsh hierarchical structure, see Chapter 2, *Understanding and Using the Traffic Management Shell*.

Alphabetical list of components

The remainder of this chapter lists the tmsh components that are available in the net ipsec module.

ike-daemon

Configures the Internet Key Exchange (ISAKMP) daemon.

Syntax

Configure the **ike-daemon** component within the **net ipsec** module using the syntax in the following sections.

Modify

```
modify ike-daemon
   description [string]
   isakmp-natt-port [port number]
   isakmp-port [port number]
   log-level [error|warning|notify|info|debug|debug2]
   natt-keep-alive [seconds]
   log-publisher [string]
```

Display

```
list
list ike-daemon
show running-config ike-daemon
    all-properties
    non-default-properties
    one-line
```

Description

You can use the **ike-daemon** component to configure global settings for the **IKE** agent.

Examples

modify ike-daemon isakmp-port 500

Sets the isakmp port to **500**.

Options

- **description**
  User defined description.
- **isakmp-natt-port**
  Specifies the port that the IKE daemon uses to accept ISAKMP messages when NAT-Traversal is detected. This is also the port number used to accept UDP-encapsulated ESP traffic for NAT-Traversal. Only **4500** is currently supported.

- **isakmp-port**
  Specifies the port that the IKE daemon uses to accept ISAKMP messages. Only **500** is currently supported.
- **log-level**
  Specifies the logging level of the IKE daemon. The log file is located at **/var/log/racoon.log**.
- **natt-keep-alive**
  Specifies the interval between sending NAT-Traversal keep-alive packets. The default value is **20** seconds. Set to **0** to disable keep-alive packets.
- **log-publisher**
  Specifies the logging publisher. A new log-publisher object can be created via TMSH command **tmsh create sys log-config publisher**.

See Also

list, *ike-peer*, *tmsh*

ike-peer

Configures one or more IKE peers for IPsec.

Syntax

Configure the **ike-peer** component within the **net ipsec** module using the syntax in the following sections.

Create/Modify

```
create ike-peer [string]
modify ike-peer [string]
   app-service [[string] | none]
   ca-cert-file [SSL certificate file]
   crl-file [SSL CRL file]
   description [string]
   dpd-delay [integer]
   generate-policy [off | on | unique ]
   lifetime [minutes]
   mode [main | aggressive]
   my-cert-file [SSL certificate file]
   my-cert-key-file [SSL certificate key file]
   my-id-type [address | asn1dn | fqdn | keyid-tag | user-fqdn]
   my-id-value [string]
   nat-traversal [on | off | force]
   passive [true | false]
   peers-cert-file [SSL certificate file]
   peers-cert-type [certfile | none]
   peers-id-type [address | asn1dn | fqdn | keyid-tag |user-fqdn]
   peers-id-value [string]
   phase1-auth-method [pre-shared-key | rsa-signature]
   phase1-encrypt-algorithm [3des | aes | blowfish | camellia | cast128 | des]
   phase1-hash-algorithm [md5 | sha1 | sha256 | sha384 | sha512]
   phase1-perfect-forward-secrecy [modp1024 | modp1536 | modp2048 | modp3072 |
modp4096 | modp6144 | modp768 | modp8192]
   preshared-key [string]
   prf [sha1 | sha256 | sha384 | sha512]
   proxy-support [disabled | enabled]
   remote-address [ip address]
   replay-window-size [integer]
   state [disabled | enabled]
   traffic-selector [name]
   verify-cert [true | false]
   version [add | delete | none | replace-all-with] {
[v1|v2]
   }
```

Display

```
list ike-peer
show running-config ike-peer
    all-properties
    non-default-properties
    one-line
show ike-peer
show ike-peer [name]
```

Delete

```
delete ike-peer [string]
```

Description

You can use the **ike-peer** component to modify the IKE phase 1 parameters for each remote **IKE** peer. The setting in the default **anonymous ike-peer** will apply to any peer that does not match a more specific **ike-peer** directive.

Examples

create ike-peer SanJose { remote-address 1.2.3.4 preshared-key abc phase1-auth-method pre-shared-key}

Creates an **ike-peer** named **SanJose** that has the IP address of **1.2.3.4** using preshared key as the authentication method.

Options

- **app-service**
  Specifies the name of the application service to which the object belongs. The default value is **none**. **Note:** If the **strict-updates** option is **enabled** on the application service that owns the object, you cannot modify or delete the object. Only the application service can modify or delete the object.
- **ca-cert-file**
  Specifies the file name of the root certificate authority.
- **crl-file**
  Specifies the file name of the **Certificate Revocation List**.
- **description**
  User-defined description.
- **dpd-delay**
  This option activates the Dead Peer Detection (DPD) and sets the time (in seconds) allowed between two proof of liveness requests. The default value is **30**. When the value is set to **0**, it means to disable DPD monitoring, but still negotiate DPD support.
- **generate_policy**
  This directive is for the responder. To use it, set **passive** to **true** so the IKE peer is only a responder. If the responder does not have any policy in the Security Policy Database (SPD) during phase 2 negotiation, and the directive is set to **on**, then the **racoon** daemon chooses the first proposal in the Security Association (SA) payload from the initiator, and generates policy entries from the proposal. It is useful to negotiate with clients whose IP address is allocated dynamically. If an inappropriate policy is installed into the responderÐØ¬ø¬¾s SPD by the initiator, other

communications might fail due to a policy mismatch between the initiator and the responder. The initiator ignores this directive. The default value is **off**.

- **lifetime**
  Specifies the lifetime of an IKE SA that will be proposed in the phase 1 negotiations.
- **mode**
  Specifies the exchange mode for phase 1 when **racoon** is the initiator, or the acceptable exchange mode when **racoon** is the responder.
- **my-cert-file**
  Specifies the name of **ssl-crt** object for the certificate file.
- **my-cert-key-file**
  Specifies the name of **ssl-key** object for the certificate key file.
- **my-id-type**
  Specifies the identifier type sent to the remote host to use in the phase 1 negotiation.
- **my-id-value**
  Specifies the identifier value sent to the remote host to use in the phase 1 negotiation.
- **nat-traversal**
  Enables use of the NAT-Traversal IPsec extension (NAT-T). NAT-T allows one or both peers to reside behind a NAT gateway (that is, performing address- or port-translation). The presence of NAT gateways along the path is discovered during the phase 1 handshake, and if found, NAT-T is negotiated. When NAT-T is in charge, all ESP and AH packets of a given connection are encapsulated into UDP datagrams (port **4500**, by default). The options are:
  - **force**
    NAT-T is used regardless of whether NAT is detected between the peers.
  - **off**
    NAT-T is not proposed/accepted. This is the default.
  - **on**
    NAT-T is used when a NAT gateway is detected between the peers.
- **passive**
  Specify **true** if you do not want to be the initiator of the IKE negotiation with this **ike-peer**.
- **peers-cert-file**
  Specifies, if **peers-cert-file** is defined, that the **isakmp** daemon ignores the CERT payload from the peer and use this certificate as the peer's certificate.
- **peers-cert-type**
  Specifies that **certfile** is the only **peers-cert-type** supported.
- **peers-id-type**
  Specifies that **address**, **fqdn**, **asn1dn**, **user-fqdn**, or **keyid-tag** can be used as **peers-id-type**.

- **peers-id-value**
  Specifies the peer's identifier to be received. If it is not defined, then the **IKE** agent will not verify the peer's identifier in the ID payload transmitted from the peer. The usage of **peers-id-type** and **peers-id-value** is the same as **my-id-type** and **my-id-value** except that the individual component values of an **asn1dn** identifier may specified as * to match any value (for example, "C=XX, O=MyOrg, OU=*, CN=Mine").
- **phase1-auth-method**
  Defines the authentication method used for the phase 1 negotiation. Possible values are: **pre-shared-key** and **rsa-signature**. Use **rsa-signature** if using X.509 certificates.
- **phase1-encrypt-algorithm**
  Specifies the encryption algorithm used for the ISAKMP phase 1 negotiation. This directive must be defined. Possible value is one of following: **des**, **3des**, **blowfish**, **cast128**, **aes**, or **camellia** for Oakley.
- **phase1-hash-algorithm**
  Defines the hash algorithm used for the ISAKMP phase 1 negotiation. This directive must be defined. The algorithm should be one of following: **md5**, **sha1**, **sha256**, **sha384**, or **sha512** for Oakley.
- **phase1-perfect-forward-secrecy**
  Defines the group used for the Diffie-Hellman exponentiations to provide perfect forward secrecy. This directive must be defined. The group is one of following: **modp768**, **modp1024**, **modp1536**, **modp2048**, **modp3072**, **modp4096**, **modp6144**, or **modp8192**.
- **preshared-key**
  Specifies the preshared key for ISAKMP SAs. This field is valid only when **phase1-auth-method** is **pre-shared-key**.
- **prf**
  Specifies the pseudo-random function to derive keying material for all cryptographic operations.
- **proxy-support**
  If this value is **enabled**, both values of ID payloads in the phase 2 exchange are used as the addresses of end-point of IPsec-SAs. This attribute must be **enabled**, which is the default value.
- **remote-address**
  Specifies the IP address of the **IKE** remote node. The format required for specifying a route domain ID in an IP address is A.B.C.D%ID. For example, A.B.C.D%2, where the IP address A.B.C.D pertains to route domain 2.

◆ Note

Route Domain is supported in case of IKE version v2 only. In all other cases, the BIG-IP system supports a default route domain with an ID of 0.

- **replay-window-size**
  Specifies the replay window size of the IPsec SAs negotiated with the **IKE** remote node. This window limits the number of out-of-order IPsec

packets that can be received relative to the packet with the higheset sequence number that has been authenticated so far. Packets with older sequence numbers that are outside this range are rejected. The default value is **64**. The valid range is from **4** to **255**.

- **state**
  Enables or disables this **IKE** remote node.
- **traffic-selector**
  Specifies the names of the **traffic-selector** objects associated with this **ike-peer**.
- **verify-cert**
  Specifies that by default, the identifier sent by the remote host (as specified in its **my_identifier** statement) is compared with the credentials in the certificate used to authenticate the remote host as follows: Type **asn1dn**: The entire certificate subject name is compared with the identifier; that is, "C=XX, O=YY," and so on. Type **address**, **fqdn**, or **user_fqdn**: The certificate's **subjectAltName** is compared with the identifier. If the two do not match, the negotiation fails. If you do not want to verify the identifier using the peer's certificate, set this to **false**.
- **version**
  Specifies which version of IKE to be used. The default value is v1. The following versions are available:
  - **v1**Specifies version IKEv1 will be used.
  - **v2**
    Specifies version IKEv2 will be used.

See Also

create, *modify*, *delete*, *list*, *tmsh*

ike-sa

Displays IKE security associations on the BIG-IP® system.

Syntax

Use the **ike-sa** component within the **ipsec** module to manage IKE security associations using the following syntax.

Display

```
show ike-sa
 option:
   all-properties
   peer-ip [IP address]
   peer-name [name]
   traffic-selector [name]
```

Description

You can use the **ike-sa** component to display information about IKE security associations in the system.

Examples

show ike-sa all-properties

Display detail information about IKE security associations.

Options

- **peer-ip**
  Specifies the peer IP address of the security associations that you want to display.
- **peer-name**
  Specifies the peer name of the security associations that you want to display.
- **traffic-selector**
  Specifies the name of the **traffic-selector** associated with the security associations that you want to display.

See Also

show

ipsec-policy

Configures the IPsec security policy.

Syntax

Configure the **ipsec-policy** component within the **net ipsec** module using the syntax in the following sections.

Create/Modify

```
create ipsec-policy [name]
modify ipsec-policy [name]
   app-service [[string] | none]
   description [string]
   ike-phase2-auth-algorithm [aes-gcm128 | aes-gcm192 | aes-gcm256 | aes-gmac128 |
aes-gmac192 | aes-gmac256 | sha1 | sha256 | sha384 | sha512]
   ike-phase2-encrypt-algorithm [3des | aes128 | aes192 | aes256 | aes-gcm128 |
aes-gcm192 | aes-gcm256 | aes-gmac128 | aes-gmac192 | aes-gmac256 | null]
   ike-phase2-lifetime [integer]
   ike-phase2-lifetime-kilobytes [integer]
   ike-phase2-perfect-forward-secrecy [modp1024 | modp1536 | modp2048 | modp3072 |
modp4096 | modp6144 | modp768 | modp8192]
   ipcomp [deflate| none | null]
   mode [transport | tunnel | isession]
   protocol [esp]
   tunnel-local-address [ip address]
   tunnel-remote-address [ip address]
```

Display

```
list ipsec-policy
list ipsec-policy
list ipsec-policy [ [ [name] | [glob] | [regex] ] ... ]
show running-config ipsec-policy
show running-config ipsec-policy [ [ [name] | [glob] | [regex] ] ... ]
   all-properties
   non-default-properties
   partition
show ipsec-policy
show ipsec-policy [name]
```

Display

```
show ipsec-policy [name]
```

Description

An **ipsec-policy** indicates the ipsec rule and action to be applied to the packets matched by the **traffic-selector** associated with this **ipsec-policy**.

Examples

create ipsec ipsec-policy tunnel_policy_sjc_sea { description "ipsec policy for the sjc-sea ipsec tunnel" mode tunnel tunnel-local-address 1.1.1.1 tunnel-remote-address 2.2.2.2 }

Creates the **tunnel mode** ipsec-policy **tunnel_policy_sjc_sea**.

delete ipsec ipsec-policy tunnel_policy_sjc_sea

Deletes the ipsec-policy **tunnel_policy_sjc_sea**.

Options

- **app-service**
  Specifies the name of the application service to which the object belongs. The default value is **none**. **Note:** If the **strict-updates** option is **enabled** on the application service that owns the object, you cannot modify or delete the object. Only the application service can modify or delete the object.
- **description**
  User defined description.
- **ike-phase2-auth-algorithm**
  Specifies a payload authentication algorithm for ESP. This attribute is only valid when IKE is used to negotiate Security Associations. The possible options are: **aes-gcm128**, **aes-gcm192**, **aes-gcm256**, **aes-gmac128**, **aes-gmac192**, **aes-gmac256**, **sha256**, **sha384**, **sha512** and **sha1**. The default value is **aes-gcm128**.

◆ Note

*Because **aes-gcm** and **aes-gmac** are authenticated encryption algorithms, when **ike-phase2-auth-algorithm** is set to **aes-gcm** or **aes-gmac**, **ike-phase2-encrypt-algorithm** has to be set to the identical algorithm with the same key length. **sha256**, **sha384**, **sha512** and **sha1** can only be used with an encryption algorithm that is **NOT** an authenticated encryption algorithm.*

- **ike-phase2-encrypt-algorithm**
  Specifies an encryption algorithm for ESP. This attribute is only valid when IKE is used to negotiate security associations. The default value is **aes-gcm128**.

◆ Note

*Because **aes-gcm** and **aes-gmac** are authenticated encryption algorithms, when **ike-phase2-encrypt-algorithm** is set to one of these algorithms, **ike-phase2-auth-algorithm** has to be set to the identical algorithm with the same key length.*

- **ike-phase2-lifetime**
  Specifies the lifetime duration in minutes, for the dynamically-negotiated security associations (SA). This attribute is only valid when IKE is used to negotiate security associations.
- **ike-phase2-lifetime-kilobytes**
  Specifies the lifetime duration in kilobytes, for the dynamically-negotiated security associations (SA). This attribute is only valid when IKE is used to negotiate security associations. A value of ‘0’ means the SA will not re-key based on the number of bytes encrypted/decrypted. The minimum recommended value is 1000 kilobytes. This value is not negotiated between peers."
- **ike-phase2-perfect-forward-secrecy**
  Defines the group of Diffie-Hellman exponentiations. This attribute is only valid when IKE is used to negotiate Security Associations. The value ‘none’ indicates that the PFS is disabled for phase2 SA negotiations.
- **mode**
  Specifies a security protocol mode for use. The options are:
  - **transport**
    IPsec **transport** mode is used.
  - **tunnel**
    IPsec **tunnel** mode is used.
  - **isession**
    A special **tunnel** mode **ipsec-policy** that is only applicable on **wom**, **remote-endpoint**, or **local-endpoint**.
- **protocol**
  Specifies the IPsec protocol: Encapsulating Security Payload (**ESP**) or Authentication Header (**AH**).
- **ipcomp**
  Specifies the compression algorithm for IPComp. The following codec are available:
  - **none**
    Disable IPComp
  - **deflate**
    Packets will be encapsulated with IPComp header and Deflate compression algorithm will be applied to the data.
  - **null**
    Packets will be encapsulated with IPComp header but no compression algorithm will be applied to the data.

- **tunnel-local-address**
  Specifies the IP address of the local IPsec tunnel endpoint. This option is only valid when **mode** is **tunnel**. The format required for specifying a route domain ID in an IP address is A.B.C.D%ID. For example, A.B.C.D%2, where the IP address A.B.C.D pertains to route domain 2.

◆ Note

Route Domain is supported in case of IKE version v2 only. In all other cases, the BIG-IP system supports a default route domain with an ID of 0.

- **tunnel-remote-address**
  Specifies the IP address of the remote IPsec tunnel endpoint. This option is only valid when **mode** is **tunnel**. The format required for specifying a route domain ID in an IP address is A.B.C.D%ID. For example, A.B.C.D%2, where the IP address A.B.C.D pertains to route domain 2.

◆ Note

Route Domain is supported in case of IKE version v2 only. In all other cases, the BIG-IP system supports a default route domain with an ID of 0.

See Also

list, *traffic-selector*, *manual-security-association*, *tmsh*

ipsec-sa

Displays IPsec security associations on the BIG-IP® system.

Syntax

Use the **ipsec-sa** component within the **ipsec** module to manage IPsec security associations using the following syntax.

Display

```
show ipsec-sa
 option:
   all-properties
   src-addr [IP address]
   dst-addr [IP address]
   spi [integer]
   traffic-selector [name]
```

Description

You can use the **ipsec-sa** component to display information about IPsec security associations in the system.

Examples

show ipsec-sa all-properties

Display detail information about IPsec security associations.

Options

- **src-addr**
  Specifies the source IP address of the security associations that you want to display.
- **dst-addr**
  Specifies the destination IP address of the security associations that you want to display.
- **spi**
  Specifies the SPI of the security associations that you want to display.
- **traffic-selector**
  Specifies the name of the **traffic-selector** object associated with the security associations that you want to display.

See Also

show, *traffic-selector*, *ipsec-policy*, *tmsh*

manual-security-association

Configures the IPsec manual-security-association.

Syntax

Configure the **manual-security-association** component within the **net ipsec** module using the syntax in the following sections.

Create/Modify

```
create manual-security-association
modify manual-security-association
   app-service [[string] | none]
   description [string]
   auth-algorithm [sha1]
   auth-key [key]
   destination-address [ip address]
   encrypt-algorithm [3des|aes128|aes192|aes256|null]
   encrypt-key [key]
   ipsec-policy [name]
   protocol [esp]
   source-address [ip address]
   spi [number]
```

Display

```
list manual-security-association
show manual-security-association
show running-config manual-security-association
   app-service
   all-properties
   non-default-properties
   one-line
```

Delete

```
delete manual-security-association [name]
```

Description

Manually configures **Security Association Database(SAD)** entries. Because each **SA** provides data protection only for unidirectional traffic, you must configure a **manual-security-association** for traffic in each direction to establish a bidirectional **IPsec** tunnel.

Examples

create ipsec manual-security-association msa_on_dut2_transport_in { auth-key test description "manual security association on dut2 for dut1 - transport" destination-address 7.7.7.7 encrypt-key test ipsec-policy transport_policy_on_dut2 source-address 2.2.2.2 spi 1025 }

Creates a **manual-security-association** object named **msa_on_dut2_transport_in** to use IPsec to protect traffic from **2.2.2.2** to **7.7.7.7** with the authentication key **test** and the encryption key **test**. The **ipsec-policy** object named **transport_policy_on_dut2** is associated with this manually configured security association.

Options

- **app-service**
  Specifies the name of the application service to which the object belongs. The default value is **none**. **Note:** If the **strict-updates** option is **enabled** on the application service that owns the object, you cannot modify or delete the object. Only the application service can modify or delete the object.
- **auth-algorithm**
  Specifies an authentication algorithm.
- **auth-key**
  Specifies the key for the authentication algorithm.
- **auth-key-encrypted**
  Displays the encrypted auth-key.
- **description**
  User-defined description.
- **destination-address**
  Specifies the destination of the security association.
- **encrypt-algorithm**
  Specifies an encryption algorithm.
- **encrypt-key**
  Specifies the key for the encryption algorithm.
- **encrypt-key-encrypted**
  Display the encrypted encrypt-key.
- **ipsec-policy**
  Specifies the **ipsec-policy** associated with this **manual-security-association**.
- **protocol**
  Specifies the **IPsec** protocol: Encapsulating Security Payload (**ESP**) or Authentication Header (**AH**).
- **source-address**
  Specifies the source address of the security association.

- **spi**
  Specifies the **Security Parameters Index**. If this is the **Security Association(SA)** for the outbound traffic, make sure it matches the SPI of the inbound SA configured on the remote site and vice versa. SPI values between **0** and **255** are reserved for the future use by IANA and cannot be used.

See Also

list, *ipsec-policy*, *tmsh*

traffic-selector

Configures a traffic selector for IPsec.

Syntax

Configure the **traffic-selector** component within the **net ipsec** module using the syntax in the following sections.

Create/Modify

```
create traffic-selector [name]
modify traffic-selector [name]
   action [protect]
   app-service [[string] | none]
   description [string]
   destination-address [ip address/netmask]
   direction [both | in | out]
   ipsec-policy [name]
   source-address [ip address/netmask]
```

Display

```
list
list traffic-selector
```

Delete

```
B<delete traffic-selector [name]>
```

Description

You can use the **traffic-selector** component to specify which incoming traffic you want the system to protect with IPsec.

Examples

create traffic-selector sjc2sea { source-address 10.10.10.0/24 destination address 20.20.20.0/24 direction both ipsec-policy my_policy}

Creates a traffic-selector named **sjc2sea**, which has the IP address of **10.10.10.0/24** using ipsec-policy named **my_policy**.

Options

- **action**
  Specifies how the system handles traffic that matches the criteria in the traffic selector. Only **protect** is currently supported.

- **app-service**
  Specifies the name of the application service to which the object belongs. The default value is **none**. **Note:** If the **strict-updates** option is **enabled** on the application service that owns the object, you cannot modify or delete the object. Only the application service can modify or delete the object.
- **description**
  User defined description.
- **destination-address**
  Specifies the destination IP address of the traffic to be matched. The format required for specifying a route domain ID in an IP address is A.B.C.D%ID. For example, A.B.C.D%2, where the IP address A.B.C.D pertains to route domain 2.

◆ Note

Route Domain is supported in case of IKE version v2 only. In all other cases, the BIG-IP system supports a default route domain with an ID of 0.

- **direction**
  Specifies the direction of traffic to be protected with IPsec. If the **direction** is **both**, use **source-address** and **destination-address** with respect to the outbound direction. The default value is **both**.
- **ipsec-policy**
  Specifies the name of the IPsec policy to be enforced on the matched traffic.
- **source-address**
  Specifies the source IP address of the traffic to be matched. The format required for specifying a route domain ID in an IP address is A.B.C.D%ID. For example, A.B.C.D%2, where the IP address A.B.C.D pertains to route domain 2.

◆ Note

Route Domain is supported in case of IKE version v2 only. In all other cases, the BIG-IP system supports a default route domain with an ID of 0.

See Also

list, *ipsec-policy*, *tmsh*

73

net rate-shaping

- Introducing the net rate-shaping module
- Alphabetical list of components

Introducing the net rate-shaping module

You can use the tmsh components that reside within the net rate-shaping module to configure rate shaping for the network. For more information about the tmsh hierarchical structure, see Chapter 2, *Understanding and Using the Traffic Management Shell*.

Alphabetical list of components

The remainder of this chapter lists the tmsh components that are available in the net rate-shaping module.

class

Configures a rate class.

Syntax

Configure the **class** component within the **net rate-shaping** module using the syntax in the following sections.

Create/Modify

```
create class [name]
modify class [name]
    app-service [[string] | none]
    ceiling [integer]
    ceiling-percentage [integer]
    description [string]
    direction [any | to-client | to-server]
    drop-policy [ [custom drop policy name ] | fred | red | tail]
    max-burst [integer]
    parent [class name]
    queue [ [custom queue name | pfifp | sfq]
    rate [integer]
    rate-percentage [integer]
    shaping-policy [ [custom shaping policy name] | none]
edit class [ [ [name] | [glob] | [regex] ] ... ]
    all-properties
    non-default-properties
```

Display

```
list class
list class [ [ [name] | [glob] | [regex] ] ... ]
show running-config class
show running-config class [ [ [name] | [glob] | [regex] ] ... ]
    all-properties
    current-module
    non-default-properties
    one-line
show class
show class [ [ [name] | [glob] | [regex] ] ... ]
    current-module
    (default | exa | gig | kil | meg | peta | raw | tera | yotta | zetta)
```

Delete

```
delete class [all | [name] ]
```

Description

You can use the **class** component to create a rate class. A rate class lets you specify shaping properties for a specific type of traffic, such as Layer 3 traffic that specifies a certain source, destination, or service. Specifically, a rate class defines the number of bits per second that the system accepts per flow and the number of packets in a queue.

You configure rate shaping by creating a class and then assigning the class to a packet filter, a virtual server, or from within an iRule. When you configure a class, you can associate another class with the class you are configuring using the **parent** option.

You can also associate drop policies, shaping policies, and queues with a class using the **drop-policy**, **shaping-policy**, and **queue** options of the **class** component. You can associate pre-configured drop policies and queues with the class, or you can create custom drop policies, queues, and shaping policies, and then associate them with the class.

Note that if you specify a value for the **shaping-policy** option of the class, the system automatically changes the **ceiling-percentage**, **drop-policy**, **max-burst**, **queue**, and **rate-percentage** options of the class to match the values in the specified shaping policy.

Examples

create class my_class rate 10

Creates a class named **my_class** with a rate of **10**.

list class all-properties

Displays all of the properties of all of the classes.

Options

- **app-service**
  Specifies the name of the application service to which the object belongs. The default value is **none**. **Note:** If the **strict-updates** option is **enabled** on the application service that owns the object, you cannot modify or delete the object. Only the application service can modify or delete the object.
- **ceiling**
  Specifies (in bps) how far beyond the value specified for the **rate** option that traffic can flow. This number sets an absolute limit. No traffic can exceed this rate. The rate class might limit traffic throughput to the value of the **rate** option when there is high contention among siblings of a parent-child class hierarchy. The default value is the value of the **rate** option. The minimum value is **296** bps.

- **ceiling-percentage**
  Specifies the ceiling of the rate class as a percentage of the ceiling of the associated parent class. This option applies only to rate classes with an associated parent rate class. The default value is **0** (zero), which indicates that the class uses the value of the **ceiling** option.
- **description**
  User defined description.
- **direction**
  Specifies the direction of traffic to which the class is applied. The default value is **any**.
- **drop-policy**
  Specifies the name of a drop policy. You can use one of the pre-configured drop policies, or you can create a customized drop policy using the **drop-policy** component.
  The default value is **tail**, which is the simplest drop policy. The pre-configured drop policies are:
  - **fred**
    Specifies that the system uses Flow-based Random Early Detection to decide whether to drop packets based on the aggressiveness of each flow.
  - **red**
    Specifies that the system uses Random Early Detection to determine whether to drop packets to maintain the average queue length within the specified range.
  - **tail**
    Specifies that the system drops all incoming packets when the queue is full.
- **glob**
  Displays the items that match the **glob** expression. See **help glob** for a description of **glob** expression syntax.
- **max-burst**
  Specifies the maximum number of bytes that traffic can burst beyond the value of the **rate** option. The traffic may not burst higher than the value of the **ceiling** option. The default value is **0** (zero).
- **name**
  Specifies a unique name for the component. This option is required for the commands **create**, **delete**, and **modify**.
- **parent**
  Associates another class with this class. The class you are configuring (which when you configure a parent class for it becomes a child class) can borrow bandwidth from the parent class. The parent class can use any of the unused bandwidth of the child class.
- **queue**
  Specifies the queuing method. The default value is **sfq**. The pre-configured options are:

- **pfifo**
  The Priority FIFO queuing method queues all traffic under a set of five sub-queues based on the Type of Service (TOS) field of the traffic. Four of the sub-queues correspond to the four possible TOS values (Minimum delay, Maximum throughput, Maximum reliability, and Minimum cost). The fifth sub-queue represents traffic with no TOS value. The Priority FIFO method processes these five sub-queues in a way that preserves the meaning of the TOS value as much as possible. For example, a packet with the TOS value of Minimum cost might yield dequeuing to a packet with the TOS value of Minimum delay.
- **sfq**
  Stochastic Fair Queuing is a queuing method that further queues packets under a set of many FIFO sub-queues. Selecting a specific sub-queue is based on a hash of the flow address information. SFQ dequeues packets from the set of sub-queues in a Round Robin fashion. The overall effect is that fairness of dequeuing is achieved, because packets from one flow cannot occupy the queues at the exclusion of those of another flow.
  Note that if you assign a shaping policy to the class, then the queuing discipline of the class becomes that specified in the shaping policy. If you do not assign a shaping policy to the class, the default queue is **sfq**.

- **rate**
  Specifies the guaranteed throughput rate of the traffic handled by this rate class, in bits per second (bps).
- **rate-percentage**
  Specifies the rate of the rate class as a percentage of the ceiling of the associated parent class. This option applies only to rate classes with an associated parent rate class. The default value is **0** (zero), which specifies that the system uses the value of the **rate** option.
- **regex**
  Displays the items that match the regular expression. The regular expression must be preceded by an at sign (@[regular expression]) to indicate that the identifier is a regular expression. See **help regex** for a description of regular expression syntax.
- **shaping-policy**
  Specifies the name of a shaping policy. The default value is **none**.
  Note that the system automatically changes the **ceiling-percentage**, **drop-policy**, **max-burst**, **queue**, and **rate-percentage** options of this class to match the values in the specified shaping policy.

See Also

create, *delete*, *edit*, glob, *list*, *modify*, *drop-policy*, *queue*, *shaping-policy*, regex, *show*, *tmsh*

drop-policy

Configures a custom drop policy for use in rate shaping.

Syntax

Configure the **drop-policy** component within the **net rate-shaping** module using the syntax in the following sections.

Create/Modify

```
create drop-policy [name]
modify drop-policy [name]
    app-service [[string] | none]
    average-packet-size [integer]
    description [string]
    fred-max-active [integer]
    fred-max-drop [integer]
    fred-min-drop [integer]
    inverse-weight [integer]
    max-probability [integer]
    max-threshold [integer]
    min-threshold [integer]
    red-hard-limit [integer]
    type [fred | red | tail]
edit drop-policy [ [ [name] | [glob] | [regex] ] ... ]
    all-properties
    non-default-properties
```

Display

```
list drop-policy
list drop-policy [ [ [name] | [glob] | [regex] ] ... ]
show running-config drop-policy
show running-config drop-policy [ [ [name] | [glob] | [regex] ] ... ]
    all-properties
    non-default-properties
    one-line
```

Delete

```
delete drop-policy [all | [name] ]
```

Description

A drop policy tells the system when and how to drop packets when the traffic handling queue is full, if required. The system comes with three pre-configured drop policies: **fred**, **red**, and **tail**.

You can use the **drop-policy** component to create a custom drop policy, and then associate it with a class using the **drop-policy** option of the **class component**. For more information, see **net rate-shaping class**.

You can also associate a custom drop policy with a shaping policy using the **drop-policy** option of the **shaping-policy** component. For more information, see **net rate-shaping shaping-policy**.

Examples

create drop-policy my_dp

Creates a custom drop policy named **my_dp**.

list drop-policy all-properties

Displays all of the properties of all of the drop policies.

Options

- **app-service**
  Specifies the name of the application service to which the object belongs. The default value is **none**. **Note:** If the **strict-updates** option is **enabled** on the application service that owns the object, you cannot modify or delete the object. Only the application service can modify or delete the object.
- **average-packet-size**
  Specifies the average MTU (maximum transmission unit) size in the range of **0** to **10000** bytes. The default value is **0** (zero).
- **description**
  User defined description.
- **fred-max-active**
  Specifies the maximum number of flows that can be active for each queue. The range is **0** to **10000**. The default value is **0** (zero),which disables active flow limitation.
- **fred-max-drop**
  Specifies a hard drop limit in the range of **0** to **400**. The default value is **0** (zero). Setting this to a small value does not change the hard drop limit, but a higher number increases the limit.
- **fred-min-drop**
  Specifies a hard no drop limit in the range of **0** to **100**. The default value is **0** (zero). Setting this to a large value prevents packets from being dropped.
- **glob**
  Displays the items that match the **glob** expression. See **help glob** for a description of **glob** expression syntax.
- **inverse-weight**
  Specifies the weight used to calculate the average queue length. Valid values are **0**, **64**, **128**, **256**, **512**, and **1024**. The default value is **0** (zero).

- **max-probability**
  Specifies the maximum percentage probability in the range of **0** to **100** according to which packets are dropped when the average queue length is between the minimum and maximum thresholds. The default value is **0** (zero).
- **max-threshold**
  Specifies the queue length above which the system drops packets. The default value is **0** (zero).
- **min-threshold**
  Specifies the queue length below which the system does not drop packets. The default value is **0** (zero).
- **name**
  Specifies a unique name for the component. This option is required for the commands **create**, **delete**, and **modify**.
- **red-hard-limit**
  Specifies the maximum queue size in bytes. Additional packets are dropped. The default value is **0** (zero).
  This option applies only when the value of the **type** option is **red**.
- **regex**
  Displays the items that match the regular expression. The regular expression must be preceded by an at sign (@[regular expression]) to indicate that the identifier is a regular expression. See **help regex** for a description of regular expression syntax.
- **type**
  Specifies the type of drop policy. The default value is **tail**.
  The options are:
  - **fred**
    Specifies that the system uses Flow-based Random Early Detection to decide whether to drop packets based on the aggressiveness of each flow.
  - **red**
    Specifies that the system uses Random Early Detection to determine whether to drop packets to maintain the average queue length within the specified range.
  - **tail**
    Specifies that the system drops all incoming packets when the queue is full. This is the simplest drop policy.
    Note that although you could create a drop policy based on **tail**, that is already the default value of the **drop-policy** option in both the **shaping-policy** and **class** components.

See Also

create, *delete*, *edit*, glob, *list*, *modify*, *class*, *queue*, *shaping-policy*, regex, *show*, *tmsh*

queue

Configures a custom queuing method.

Syntax

Configure the **queue** component within the **net rate-shaping** module using the syntax in the following sections.

Create/Modify

```
create queue [pfifo | sfq]
modify queue [all | pfifo | sfq]
    app-service [[string] | none]
    description [string]
    pfifo-max-size [integer]
    pfifo-min-size [integer]
    sfq-bucket-count [integer]
    sfq-bucket-size [integer]
    sfq-perturbation [integer]
    type [pfifo | sfq]
edit queue [ [ [all | pfifo | sfq] | [glob] | [regex] ] ... ]
    all-properties
    non-default-properties
```

Display

```
list queue
list queue [ [ [all | pfifo | sfq] | [glob] | [regex] ] ... ]
show running-config queue
show running-config queue
  [ [ [all | pfifo | sfq] | [glob] | [regex] ] ... ]
    all-properties
    non-default-properties
    one-line
```

Delete

```
delete queue [all | [name] ]
```

Description

You can use the **queue** component to configure a custom queuing method.

Examples

create queue my_q type pfifo

Creates a pfifo type queue name **my_q**.

list queue all-properties

Displays all of the properties of all of the queue.

Options

- **app-service**
  Specifies the name of the application service to which the object belongs. The default value is **none**. **Note:** If the **strict-updates** option is **enabled** on the application service that owns the object, you cannot modify or delete the object. Only the application service can modify or delete the object.
- **description**
  User defined description.
- **glob**
  Displays the items that match the **glob** expression. See **help glob** for a description of **glob** expression syntax.
- **name**
  Specifies a unique name for the component. This option is required for the commands **create**, **delete**, and **modify**.
- **pfifo-max-size**
  Specifies the size of the largest queue for the pfifo type only. The default value is **0** (zero). Valid units are bytes(default), eb, gb, k, kb, mb, pb, and tb.
- **pfifo-min-size**
  Specifies the size of the smallest queue for the pfifo type only. The default value is **0** (zero). Valid units are bytes(default), eb, gb, k, kb, mb, pb, and tb.
- **regex**
  Displays the items that match the regular expression. The regular expression must be preceded by an at sign (@[regular expression]) to indicate that the identifier is a regular expression. See **help regex** for a description of regular expression syntax.
- **sfq-bucket-count**
  Specifies the number of buckets into which the queue is divided when you are configuring the sfq type. Valid values are 0, 16, 32, 64, 128, 256, 512, and 1024. The default value is **0** (zero).
- **sfq-bucket-size**
  Specifies the bucket size for the **sfq** type. The default value is **0** (zero). Valid units are bytes(default), eb, gb, k, kb, mb, pb, and tb.
- **sfq-perturbation**
  Specifies the interval in seconds at which the system reconfigures the SFQ hash function. This option applies only to the **sfq** type. The default value is **0** (zero).
- **type**
  Specifies the queue discipline this custom queue uses. The options are:

- **pfifo**
  The Priority FIFO queuing method queues all traffic under a set of five sub-queues based on the Type of Service (TOS) field of the traffic. Four of the sub-queues correspond to the four possible TOS values (Minimum delay, Maximum throughput, Maximum reliability, and Minimum cost). The fifth sub-queue represents traffic with no TOS value. The Priority FIFO method processes these five sub-queues in a way that preserves the meaning of the TOS value as much as possible. For example, a packet with the TOS value of Minimum cost might yield dequeuing to a packet with the TOS value of Minimum delay.
- **sfq**
  Stochastic Fair Queuing is a queuing method that further queues packets under a set of many FIFO sub-queues. Selecting a specific sub-queue is based on a hash of the flow address information. SFQ dequeues packets from the set of sub-queues in a Round Robin fashion. The overall effect is that fairness of dequeuing is achieved, because packets from one flow cannot occupy the queues at the exclusion of those of another flow.

See Also

create, *delete*, *edit*, glob, *list*, *modify*, *class*, *drop-policy*, *shaping-policy*, regex, *show*, *tmsh*

shaping-policy

Configures a custom rate shaping policy for traffic flow.

Syntax

Configure the **shaping-policy** component within the **net rate-shaping** module using the syntax in the following sections.

Create/Modify

```
create shaping-policy [name]
modify shaping-policy [name]
    app-service [[string] | none]
    ceiling-percentage [integer]
    description [string]
    drop-policy [ [name] | none]
    max-burst [integer]
    queue [ [name] | none]
    rate-percentage [integer]
edit shaping-policy [ [ [name] | [glob] | [regex] ] ... ]
    all-properties
    non-default-properties
```

Display

```
list shaping-policy
list shaping-policy [ [ [name] | [glob] | [regex] ] ... ]
show running-config shaping-policy
show running-config shaping-policy [ [ [name] | [glob] | [regex] ] ... ]
    all-properties
    non-default-properties
    one-line
```

Delete

```
delete shaping-policy [all | [name] ]
```

Description

You can use the **shaping-policy** component to create a custom rate shaping policy to handle traffic flow, and then associate the shaping policy with a class.

Note that if you specify a value for the **shaping-policy** option of a class, the system automatically changes the **ceiling-percentage**, **drop-policy**, **max-burst**, **queue**, and **rate-percentage** options of that class to match the values in the shaping policy.

Examples

create shaping-policy my_sp

Creates a shaping policy named **my_sp**.

list shaping policies all-properties

Displays all of the properties of all of the shaping policies.

Options

- **app-service**
  Specifies the name of the application service to which the object belongs. The default value is **none**. **Note:** If the **strict-updates** option is **enabled** on the application service that owns the object, you cannot modify or delete the object. Only the application service can modify or delete the object.
- **ceiling-percentage**
  Specifies the percentage of the value of the **ceiling** option specified for the parent associated with the **class** component to which this shaping policy is associated. The default value is **0** (zero).
- **description**
  User defined description.
- **drop-policy**
  Specifies the name of a drop policy for this traffic flow. The default value is **none**.
  You can use one of the pre-configured drop policies, or you can create a customized drop-policy using the **drop-policy** component.
  The pre-configured drop policies are:
  - **fred**
    Specifies that the system uses Flow-based Random Early Detection to decide whether to drop packets based on the aggressiveness of each flow.
  - **red**
    Specifies that the system uses Random Early Detection to determine whether to drop packets to maintain the average queue length within the specified range.
  - **tail**
    Specifies that the system drops all incoming packets when the queue is full. This is the simplest drop policy.
- **glob**
  Displays the items that match the **glob** expression. See **help glob** for a description of **glob** expression syntax.
- **max-burst**
  Specifies the maximum number of bytes that traffic is allowed to burst beyond the value of the **rate** option of the **class** component to which this shaping policy is associated. The default value is **0** (zero).
  Valid units are byte, bytes(default), eb, gb, k, kb, mb, pb, and tb.

- **name**
  Specifies a unique name for the component. This option is required for the commands **create**, **delete**, and **modify**.
- **queue**
  Specifies the queuing method for this traffic flow. The default value is **none**. You can create a customized queuing method using the **queue** component. For more information, see **net rate-shaping queue**.
  The preconfigured queues are:
  - **pfifo**
    The Priority FIFO queuing method queues all traffic under a set of five sub-queues based on the Type of Service (TOS) field of the traffic. Four of the sub-queues correspond to the four possible TOS values (Minimum delay, Maximum throughput, Maximum reliability, and Minimum cost). The fifth sub-queue represents traffic with no TOS value. The Priority FIFO method processes these five sub-queues in a way that preserves the meaning of the TOS value as much as possible. For example, a packet with the TOS value of Minimum cost might yield dequeuing to a packet with the TOS value of Minimum delay.
  - **sfq**
    Stochastic Fair Queuing is a queuing method that further queues packets under a set of many FIFO sub-queues. Selecting a specific sub-queue is based on a hash of the flow address information. SFQ dequeues packets from the set of sub-queues in a Round Robin fashion. The overall effect is that fairness of dequeuing is achieved, because packets from one flow cannot occupy the queues at the exclusion of those of another flow.
- **rate-percentage**
  Specifies the percentage of the value of the **rate** option of the parent, which is associated with the **class** component to which this shaping policy is associated, that is available for this traffic flow. The default value is **0** (zero).
- **regex**
  Displays the items that match the regular expression. The regular expression must be preceded by an at sign (@[regular expression]) to indicate that the identifier is a regular expression. See **help regex** for a description of regular expression syntax.

See Also

create, *delete*, *edit*, glob, *list*, *modify*, *drop-policy*, *queue*, *shaping-policy*, regex, *show*, *tmsh*

74

net tunnels

- Introducing the net tunnels module
- Alphabetical list of components

Introducing the net tunnels module

You can use the tmsh components that reside within the net tunnels module to configure tunnels for the BIG-IP® system. For more information about the tmsh hierarchical structure, see Chapter 2, *Understanding and Using the Traffic Management Shell*.

Alphabetical list of components

The remainder of this chapter lists the tmsh components that are available in the net tunnels module.

etherip

Configures an EtherIP tunnel profile.

Syntax

Configure the **etherip** component within the **net tunnels** module using the syntax in the following sections.

Create/Modify

```
create etherip [name]
modify etherip [name]
    app-service [[string] | none]
    defaults-from [name]
    description [string]
edit etherip [ [ [name] | [glob] | [regex] ] ... ]
    all-properties
    non-default-properties
```

Display

```
list etherip
list etherip [ [ [name] | [glob] | [regex] ] ... ]
show running-config etherip
show running-config etherip [ [ [name] | [glob] | [regex] ] ... ]
    all-properties
    app-service
    non-default-properties
    one-line
    partition
```

Delete

```
delete etherip [ all | [name] ]
```

Description

You can use the **etherip** component to create an EtherIP profile that you associate with a tunnel using the **tunnel** component. This will cause ethernet frames to be sent over the tunnel. For more information about creating a tunnel see **net tunnel**.

Examples

create etherip my_etherip

Creates an EtherIP profile called **my_etherip**.

list etherip all-properties

Displays all of the properties of all EtherIP profiles.

Options

- **app-service**
  Specifies the name of the application service to which the object belongs. The default value is **none**. **Note:** If the **strict-updates** option is **enabled** on the application service that owns the object, you cannot modify or delete the object. Only the application service can modify or delete the object.
- **defaults-from**
  Specifies the existing profile from which the system imports settings for the new profile. The default value is **etherip**.
- **description**
  User defined description.
- **glob**
  Displays the items that match the **glob** expression. See **help glob** for a description of **glob** expression syntax.
- **name**
  Specifies a unique name for the component. This option is required for the commands **create** and **modify**.
- **partition**
  Displays the administrative partition within which this component resides.
- **regex**
  Displays the items that match the regular expression. The regular expression must be preceded by an at sign (@[regular expression]) to indicate that the identifier is a regular expression. See **help regex** for a description of regular expression syntax.

See Also

create, *delete*, *edit*, glob, *list*, *modify*, *tunnel*, regex, *show*, *tmsh*

fec

Configures a Forward Error Correction (FEC) profile.

Syntax

Configure the **fec** component within the **net tunnels** module using the syntax in the following sections.

Create/Modify

```
create fec [name]
modify fec [name]
    app-service [[string] | none]
    decode-idle-timeout [integer]
    decode-max-packets [integer]
    decode-queues [integer]
    defaults-from [name]
    description [string]
    encode-max-delay [integer]
    keepalive-interval [integer]
    lzo [disabled | enabled]
    repair-adaptive [disabled | enabled]
    repair-packets [integer]
    source-adaptive [disabled | enabled]
    source-packets [integer]
    udp-port [integer]
edit fec [ [ [name] | [glob] | [regex] ] ... ]
    all-properties
    non-default-properties
=head2 DISPLAY
list fec
list fec [ [ [name] | [glob] | [regex] ] ... ]
show running-config fec
show running-config fec [ [ [name] | [glob] | [regex] ] ... ]
    all-properties
    app-service
    non-default-properties
    one-line
    partition
```

Delete

```
delete fec [ all | [name] ]
```

Description

You can use the **fec** component to create a FEC profile that you associate with a tunnel using the **tunnel** component. For more information about creating a tunnel see **net tunnel**.

Examples

create fec my_fec

Creates a FEC profile called **my_fec**.

list fec all-properties

Displays all of the properties of all of the FEC profiles.

Options

- **app-service**
  Specifies the name of the application service to which the object belongs. The default value is **none**. **Note:** If the **strict-updates** option is **enabled** on the application service that owns the object, you cannot modify or delete the object. Only the application service can modify or delete the object.
- **defaults-from**
  Specifies the existing profile from which the system imports settings for the new profile. The default value is **fec**.
- **description**
  User defined description.
- **glob**
  Displays the items that match the **glob** expression. See **help glob** for a description of **glob** expression syntax.
- **name**
  Specifies a unique name for the component. This option is required for the commands **create** and **modify**.
- **partition**
  Displays the administrative partition within which this component resides.
- **regex**
  Displays the items that match the regular expression. The regular expression must be preceded by an at sign (@[regular expression]) to indicate that the identifier is a regular expression. See **help regex** for a description of regular expression syntax.
- **decode-idle-timeout**
  Specifies the maximum waiting time for packets in decoding queues. Packets waiting longer than this time are discarded. Range is from **250** to **2000** milliseconds. The default value is **1500** milliseconds.
- **decode-max-packets**
  Specifies the maximum number of waiting packets in decoding queues. Range is from **200** to **8000**. The default value is **512**.
- **decode-queues**
  Specifies the number of decoding queues. Valid numbers are **8**, **16**, **32**, **64**, **128**, **256**, **512**, **1024**. The default value is **32**.

- **encode-max-delay**
  Specifies the maximum waiting time for packet aggregation. Range is from **500** to **5000** microseconds. The default value is **500** microseconds.
- **keepalive-interval**
  Specifies the interval between keepalive (statistical data) packets. Range is from **0** to **100** seconds. The default value is **5** seconds.
- **lzo**
  Controls the use of the LZO compression algorithm to compress data packets. The default value is **enabled**.
- **repair-adaptive**
  Controls the use of the adaptive FEC repair technique to modify the number of redundant packets according to actual network conditions. The default value is **enabled**.
- **repair-packets**
  Specifies the number of redundant packets to add. Range is from **0** to **15**. The default value is **15**. This value should be less than or equal to the value specified for **source-packets**.
- **source-adaptive**
  Controls the use of the adaptive FEC source packets technique to reduce the number of packets for better MTU usage. The default value is **enabled**.
- **source-packets**
  Specifies the number of packets into which the system divides the aggregated payload. Range is from **1** to **15**. The default value is **15**.
- **udp-port**
  Specifies the local port for receiving FEC packets. The default value is **8288**.

See Also

create, *delete*, *edit*, glob, *list*, *modify*, *ipip*, *tunnel*, *wccp*, regex, *show*, *tmsh*

gre

Configures a Generic Router Encapsulation (GRE) profile.

Syntax

Configure the **gre** component within the **net tunnels** module using the syntax in the following sections.

Create/Modify

```
create gre [name]
modify gre [name]
    app-service [[string] | none]
    defaults-from [name]
    description [string]
    rx-csum [disabled | enabled]
    tx-csum [disabled | enabled]
    encapsulation [standard | nvgre]
    flooding-type [none | multipoint]
edit gre [ [ [name] | [glob] | [regex] ] ... ]
    all-properties
    non-default-properties
```

Display

```
list gre
list gre [ [ [name] | [glob] | [regex] ] ... ]
show running-config gre
show running-config gre [ [ [name] | [glob] | [regex] ] ... ]
    all-properties
    app-service
    non-default-properties
    one-line
    partition
```

Delete

```
delete gre [ all | [name] ]
```

Description

You can use the **gre** component to create a GRE profile that you associate with a tunnel using the **tunnel** component. For more information about creating a tunnel see **net tunnel**.

Examples

create gre my_gre

Creates a GRE profile called **my_gre**.

list gre all-properties

Displays all of the properties of all of the GRE profiles.

Options

- **app-service**
  Specifies the name of the application service to which the object belongs. The default value is **none**. **Note:** If the **strict-updates** option is **enabled** on the application service that owns the object, you cannot modify or delete the object. Only the application service can modify or delete the object.
- **defaults-from**
  Specifies the existing profile from which the system imports settings for the new profile. The default value is **gre**.
- **description**
  User defined description.
- **glob**
  Displays the items that match the **glob** expression. See **help glob** for a description of **glob** expression syntax.
- **name**
  Specifies a unique name for the component. This option is required for the commands **create** and **modify**.
- **partition**
  Displays the administrative partition within which this component resides.
- **regex**
  Displays the items that match the regular expression. The regular expression must be preceded by an at sign (@[regular expression]) to indicate that the identifier is a regular expression. See **help regex** for a description of regular expression syntax.
- **rx-csum**
  Specifies whether the system verifies the checksum on received packets. The default value is **disabled**.
- **tx-csum**
  Specifies whether the system includes a checksum on transmitted packets. The default value is **disabled**.
- **encapsulation**
  Specifies the flavor of GRE header to use for encapsulation. The default value is **standard**.
- **flooding-type**
  Specifies the flooding type to use to transmit broadcast and unknown destination frames. The default is **none**.

See Also

create, *delete*, *edit*, glob, *list*, *modify*, *ipip*, *tunnel*, *wccp*, regex, *show*, *tmsh*

ipip

Configures an IP over IP (IPIP) profile.

Syntax

Configure the **ipip** component within the **net tunnels** module using the syntax in the following sections.

Create/Modify

```
create ipip [name]
modify ipip [name]
    app-service [[string] | none]
    defaults-from [name]
    description [string]
    proto [IPv4 | IPv6]
    ds-lite [bool]
edit ipip [ [ [name] | [glob] | [regex] ] ... ]
    all-properties
    non-default-properties
```

Display

```
list ipip
list ipip [ [ [name] | [glob] | [regex] ] ... ]
show running-config ipip
show running-config ipip [ [ [name] | [glob] | [regex] ] ... ]
    all-properties
    app-service
    non-default-properties
    one-line
    partition
```

Delete

```
delete ipip [ all | [name] ]
```

Description

You can use the **ipip** component to create an IPIP profile that you associate with a tunnel using the **tunnel** component. For more information about creating a tunnel see **net tunnel**.

Examples

create ipip my_ipip

Creates an IPIP profile called **my_ipip**.

list ipip all-properties

Displays all of the properties of all of the IPIP profiles.

Options

- **app-service**
  Specifies the name of the application service to which the object belongs. The default value is **none**. **Note:** If the **strict-updates** option is **enabled** on the application service that owns the object, you cannot modify or delete the object. Only the application service can modify or delete the object.
- **defaults-from**
  Specifies the existing profile from which the system imports settings for the new profile. The default value is **ipip**.
- **description**
  User defined description.
- **glob**
  Displays the items that match the **glob** expression. See **help glob** for a description of **glob** expression syntax.
- **name**
  Specifies a unique name for the component. This option is required for the commands **create** and **modify**.
- **partition**
  Displays the partition within which this component resides.
- **proto**
  Specifies the next header protocol. The default value is **IPv4**.
- **regex**
  Displays the items that match the regular expression. The regular expression must be preceded by an at sign (@[regular expression]) to indicate that the identifier is a regular expression. See **help regex** for a description of regular expression syntax.
- **ds-lite**
  Specifies whether the profile is used for a DS-lite deployment. When enabled, an augmented flow lookup is made using the IPv6 address in the outer header in addition to the inner header addresses for packets coming over this tunnel. The default value is **disabled**.

See Also

create, *delete*, *edit*, glob, *list*, *modify*, *gre*, *tunnel*, *wccp*, regex, *show*, *tmsh*

ipsec

Configures an IPsec profile.

Syntax

Configure the **ipsec** component within the **net tunnels** module using the syntax in the following sections.

Create/Modify

```
create ipsec [name]
modify ipsec [name]
    app-service [[string] | none]
    defaults-from [ [name] | none]
    description [string]
    traffic-selector [name]
edit ipsec [ [ [name] | [glob] | [regex] ] ... ]
    all-properties
    non-default-properties
```

Display

```
list ipsec
list ipsec [ [ [name] | [glob] | [regex] ] ... ]
show running-config ipsec
show running-config ipsec [ [ [name] | [glob] | [regex] ] ... ]
    all-properties
    app-service
    non-default-properties
    one-line
    partition
```

Delete

```
delete ipsec [ all | [name] ]
```

Description

You can use the **ipsec** component to create an ipsec profile that you associate with a tunnel using the **tunnel** component. For more information about creating a tunnel see **net tunnel**.

Examples

create ipsec my_ipsec

Creates an IPsec profile called **my_ipsec**.

list ipsec all-properties

Displays all the properties of all the IPsec profiles.

Options

- **app-service**
  Specifies the name of the application service to which the object belongs. The default value is **none**. **Note:** If the **strict-updates** option is **enabled** on the application service that owns the object, you cannot modify or delete the object. Only the application service can modify or delete the object.
- **defaults-from**
  Specifies the existing profile from which the system imports settings for the new profile. The default value is **ipsec**.
- **description**
  User defined description.
- **glob**
  Displays the items that match the **glob** expression. See **help glob** for a description of **glob** expression syntax.
- **name**
  Specifies a unique name for the component. This option is required for the commands **create** and **modify**.
- **partition**
  Displays the administrative partition within which this component resides.
- **traffic-selector**
  Specifies the IPsec traffic selector for the IPsec tunnel.
- **regex**
  Displays the items that match the regular expression. The regular expression must be preceded by an at sign (@[regular expression]) to indicate that the identifier is a regular expression. See **help regex** for a description of regular expression syntax.

See Also

create, *delete*, *edit*, glob, *list*, *modify*, *tunnel*, regex, *show*, *tmsh*

map

Configures a MAP tunnel profile.

Syntax

Configure the **map** component within the **net tunnels** module using the syntax in the following sections.

Create/Modify

```
create map [name]
modify map [name]
    app-service [[string] | none]
    defaults-from [ [name] | none]
    description [string]
    ip6-prefix [ipv6 address/prefix length]
    ip4-prefix [ipv4 address/prefix length]
    ea-bits-length [integer]
    port-offset [integer]
edit map [ [ [name] | [glob] | [regex] ] ... ]
    all-properties
    non-default-properties
```

Display

Delete

```
delete map [ all | [name] ]
```

Description

You can use the **map** component to create a MAP profile that you associate with a tunnel using the **tunnel** component. For more information about creating a tunnel see **net tunnel**.

Examples

create map my_map

Creates a MAP profile called **my_map**.

list map all-properties

Displays all the properties of all the MAP profiles.

Options

- **app-service**
  Specifies the name of the application service to which the object belongs. The default value is **none**. **Note:** If the **strict-updates** option is **enabled** on the application service that owns the object, you cannot modify or delete the object. Only the application service can modify or delete the object.
- **defaults-from**
  Specifies the existing profile from which the system imports settings for the new profile. The default value is **map**.
- **description**
  User defined description.
- **glob**
  Displays the items that match the **glob** expression. See **help glob** for a description of **glob** expression syntax.
- **name**
  Specifies a unique name for the component. This option is required for the commands **create** and **modify**.
- **partition**
  Displays the administrative partition within which this component resides.
- **regex**
  Displays the items that match the regular expression. The regular expression must be preceded by an at sign (@[regular expression]) to indicate that the identifier is a regular expression. See **help regex** for a description of regular expression syntax.
- **ip6-prefix**
  Specifies the IPv6 Prefix using CIDR notation, such as **2014::/48**. The default prefix length is 48.
- **ip4-prefix**
  Specifies the IPv4 Prefix using CIDR notation, such as **192.0.0.0/8**. The default prefix length is 8.
- **ea-bits-length**
  Specifies the length in bits of the EA (Embedded Address) of the MAP domain. The default is 32 (IPv4 prefix 24 bits + PSID 8 bits).
- **port-offset**
  Specifies the port offset bits length of the MAP domain. The default is 6.

See Also

create, *delete*, *edit*, glob, *list*, *modify*, *tunnel*, regex, *show*, *tmsh*

PPP

Configures a PPP profile.

Syntax

Configure the **ppp** component within the **net tunnels** module using the syntax in the following sections.

Create/Modify

```
create ppp [name]
modify ppp [name]
    app-service [[string] | none]
    defaults-from [ [name] | none]
    description [string]
    lcp-echo-failure [integer]
    lcp-echo-interval [integer]
    vj [disabled | enabled]
edit ppp [ [ [name] | [glob] | [regex] ] ... ]
    all-properties
    non-default-properties
```

Display

```
list ppp
list ppp [ [ [name] | [glob] | [regex] ] ... ]
show running-config ppp
show running-config ppp [ [ [name] | [glob] | [regex] ] ... ]
    all-properties
    app-service
    non-default-properties
    one-line
    partition
```

Delete

```
delete ppp [ all | [name] ]
```

Description

You can use the **ppp** component to create a ppp profile that you associate with a tunnel using the **tunnel** component. For more information about creating a tunnel see **net tunnel**.

Examples

create ppp my_ppp

Creates a PPP profile called **my_ppp**.

list ppp all-properties

Displays all the properties of all the PPP profiles.

Options

- **app-service**
  Specifies the name of the application service to which the object belongs. The default value is **none**. **Note:** If the **strict-updates** option is **enabled** on the application service that owns the object, you cannot modify or delete the object. Only the application service can modify or delete the object.
- **defaults-from**
  Specifies the existing profile from which the system imports settings for the new profile. The default value is **ppp**.
- **description**
  User defined description.
- **glob**
  Displays the items that match the **glob** expression. See **help glob** for a description of **glob** expression syntax.
- **lcp-echo-failure**
  Specifies the number of consecutive PPP LCP echo messages that must go unanswered for the server to drop PPP connection. For example, if the server sends **number** of consecutive PPP LCP Echo Request messages that go unanswered (by Echo Reply), it will close the PPP connection. The default value is **4**.
- **lcp-echo-interval**
  Specifies the interval, in seconds, between the PPP LCP Echo Request messages that the server sends to the peer (client). The default value is **30**.
- **name**
  Specifies a unique name for the component. This option is required for the commands **create** and **modify**.
- **partition**
  Displays the administrative partition within which this component resides.
- **regex**
  Displays the items that match the regular expression. The regular expression must be preceded by an at sign (@[regular expression]) to indicate that the identifier is a regular expression. See **help regex** for a description of regular expression syntax.
- **vj**
  Specifies whether the system uses Van Jacobson Header Compression (also known as VJ compression, or just Header Compression), which is an option in most versions of PPP. VJ is a data compression protocol described in RFC 1144, specifically designed by Van Jacobson to improve TCP/IP performance over slow serial links. The default value is **disabled**.

See Also

create, *delete*, *edit*, glob, *list*, *modify*, *tunnel*, regex, *show*, *tmsh*

tunnel

Configures a tunnel.

Syntax

Configure the **tunnel** component within the **net tunnels** module using the syntax in the following sections.

Create/Modify

```
create tunnel [name]
modify tunnel [name]
     app-service [[string] | none]
     auto-lasthop [default | enabled | disabled ]
     description [string]
     local-address [ip address]
     mode [bidirectional | inbound | outbound]
     mtu [integer]
     use-pmtu [enabled | disabled ]
     profile [name]
     remote-address [ip address]
     tos [integer]
     transparent [enabled | disabled ]
     idle-timeout [integer]
     key [integer]
edit tunnel [ [ [name] | [glob] | [regex] ] ... ]
    all-properties
    non-default-properties
```

Display

```
list tunnel
list tunnel [ [ [name] | [glob] | [regex] ] ... ]
show running-config tunnel
show running-config tunnel [ [ [name] | [glob] | [regex] ] ... ]
    all-properties
    app-service
    non-default-properties
    one-line
    partition
```

Delete

```
delete tunnel [ all | [name] ]
```

Description

You can use the **tunnel** component to configure a tunnel.

Examples

create tunnel my_tunnel local-address 10.10.10.1 remote-address 11.11.11.1 profile gre

Creates a tunnel named **my_tunnel** between the local IP address **10.10.10.1** and the remote IP address **11.11.11.1**.

list tunnel all-properties

Displays all of the properties of all of the tunnels.

Options

- **app-service**
  Specifies the name of the application service to which the object belongs. The default value is **none**. **Note:** If the **strict-updates** option is **enabled** on the application service that owns the object, you cannot modify or delete the object. Only the application service can modify or delete the object.
- **auto-lasthop**
  When enabled, specifies that the system returns packets to the MAC address from which they were sent. The default setting is **default**, which specifies that the system uses the default route to send back the request.
- **description**
  User defined description.
- **glob**
  Displays the items that match the **glob** expression. See **help glob** for a description of **glob** expression syntax.
- **local-address**
  Specifies a local IP address. This option is required.
- **mode**
  Specifies how the tunnel carries traffic. The default value is **bidirectional**.
- **mtu**
  Specifies the maximum transmission unit (MTU) of the tunnel. The default value is 0. When the MTU is set to the default value (of 0), the MTU of the tunnel is computed by the system and is set to the MTU size of the underlying interface minus the encapsulation overhead introduced by the tunneling protocol. The valid range is **0** - **65535**.
- **use-pmtu**
  Enables or disables the tunnel to use the PMTU (Path MTU) information provided by ICMP NeedFrag error messages. If enabled and the tunnel MTU is set to 0, the tunnel will use the PMTU information. If enabled and the tunnel MTU is fixed to a non-zero value, the tunnel will use the minimum of PMTU and MTU. If disabled, the tunnel will use fixed MTU, or calculate its MTU using tunnel encapsulation configurations.
- **name**
  Specifies a unique name for the component. This option is required for the commands **create**, and **modify**.

- **partition**
  Displays the administrative partition within which the component resides.
- **profile**
  Specifies the profile that you want to associate with the tunnel. This option is required for the **create** command.
- **regex**
  Displays the items that match the regular expression. The regular expression must be preceded by an at sign (@[regular expression]) to indicate that the identifier is a regular expression. See **help regex** for a description of regular expression syntax.
- **remote-address**
  Specifies a remote IP address. This value is required for the commands **create** and **modify**.
- **tos**
  Specifies a value for insertion into the Type of Service (ToS) octet within the IP header of the encapsulating header of transmitted packets. The default value is **preserve**. The possible values are **0** (zero) - **255**.
- **transparent**
  Enables or disables the tunnel to be transparent. If enabled, the user can inspect and/or manipulate the encapsulated traffic flowing through the BIG-IP. A transparent tunnel terminates a tunnel while presenting the illusion that the tunnel transits the device unperturbed i.e. the BIG-IP appears like an intermediate router that simply routes IP traffic through the device. The default value is **disabled**.
- **idle-timeout**
  Specifies an idle timeout for wildcard tunnels in seconds. This setting specifies the number of seconds that a wildcard tunnel connection is idle before the connection is eligible for deletion. The default value is **300 seconds**.
- **key**
  The key field may represent different values depending on the type of the tunnel. For VXLAN it represents the Virtual Network Identifier (VNI). The default value is **0**.

See Also

create, *delete*, *edit*, glob, *list*, *modify*, *gre*, *ipip*, *wccp*, regex, *show*, *tmsh*

v6rd

Configures a 6RD profile.

Syntax

Configure the **v6rd** component within the **net tunnels** module using the syntax in the following sections.

Create/Modify

```
create v6rd [name]
modify v6rd [name]
    app-service [[string] | none]
    defaults-from [ [name] | none]
    description [string]
    v6rdprefix [IPv6 address]
    v6rdprefixlen [integer]
    ipv4prefix [IPv4 address]
    ipv4prefixlen [integer]
edit v6rd [ [ [name] | [glob] | [regex] ] ... ]
    all-properties
    non-default-properties
```

Display

Delete

```
delete v6rd [ all | [name] ]
```

Description

You can use the **v6rd** component to create a v6rd profile that you associate with a tunnel using the **tunnel** component. For more information about creating a tunnel see **net tunnel**.

Examples

create v6rd my_v6rd

Creates a 6RD profile called **my_v6rd**.

list v6rd all-properties

Displays all the properties of all the 6RD profiles.

Options

- **app-service**
  Specifies the name of the application service to which the object belongs. The default value is **none**. **Note:** If the **strict-updates** option is **enabled** on the application service that owns the object, you cannot modify or delete the object. Only the application service can modify or delete the object.
- **defaults-from**
  Specifies the existing profile from which the system imports settings for the new profile. The default value is **v6rd**.
- **description**
  User defined description.
- **glob**
  Displays the items that match the **glob** expression. See **help glob** for a description of **glob** expression syntax.
- **name**
  Specifies a unique name for the component. This option is required for the commands **create** and **modify**.
- **partition**
  Displays the administrative partition within which this component resides.
- **regex**
  Displays the items that match the regular expression. The regular expression must be preceded by an at sign (@[regular expression]) to indicate that the identifier is a regular expression. See **help regex** for a description of regular expression syntax.
- **v6rdprefix**
  Specifies the IPv6 prefix for 6rd domain.
- **v6rdprefixlen**
  Specifies the IPv6 prefix length of the 6rd domain. The default is 56.
- **ipv4prefix**
  As an extension not mentioned in the RFC5969, it specifies the IPv4 prefix for the Customer-Edge (CE) devices of a 6RD domain at a Border-Relay (BR) in case that the subnet prefixes used by the 6RD devices do not share the same IPv4 prefix. If they do, there is no need to configure this parameter. The default value is **0.0.0.0**.
- **ipv4prefixlen**
  Also noted as IPv4MaskLen in RFC5969, it specifies the number of identical high-order bits shared by all CE and BR IPv4 addresses in a given 6RD domain. The valid range is from zero to 32. It is a required value for create. It defaults to zero, i.e. the full ipv4 address must be encapsulated.

See Also

create, *delete*, *edit*, glob, *list*, *modify*, *tunnel*, regex, *show*, *tmsh*

vxlan

Configures a VXLAN profile.

Syntax

Configure the **vxlan** component within the **net tunnels** module using the syntax in the following sections.

Create/Modify

```
create vxlan [name]
modify vxlan [name]
    app-service [[string] | none]
    defaults-from [ [name] | none]
    description [string]
    port [integer]
    flooding-type [none | multicast | multipoint]
edit vxlan [ [ [name] | [glob] | [regex] ] ... ]
    all-properties
    non-default-properties
```

Display

```
list vxlan
list vxlan [ [ [name] | [glob] | [regex] ] ... ]
show running-config vxlan
show running-config vxlan [ [ [name] | [glob] | [regex] ] ... ]
    all-properties
    app-service
    non-default-properties
    one-line
    partition
```

Delete

```
delete vxlan [ all | [name] ]
```

Description

You can use the **vxlan** component to create a vxlan profile that you associate with a tunnel using the **tunnel** component. For more information about creating a tunnel see **net tunnel**.

Examples

create vxlan my_vxlan

Creates a VXLAN profile called **my_vxlan**.

list vxlan all-properties

Displays all the properties of all the VXLAN profiles.

Options

- **app-service**
  Specifies the name of the application service to which the object belongs. The default value is **none**. **Note:** If the **strict-updates** option is **enabled** on the application service that owns the object, you cannot modify or delete the object. Only the application service can modify or delete the object.
- **defaults-from**
  Specifies the existing profile from which the system imports settings for the new profile. The default value is **vxlan**.
- **description**
  User defined description.
- **glob**
  Displays the items that match the **glob** expression. See **help glob** for a description of **glob** expression syntax.
- **name**
  Specifies a unique name for the component. This option is required for the commands **create** and **modify**.
- **partition**
  Displays the administrative partition within which this component resides.
- **port**
  Specifies the local port for receiving VXLAN packets. The default is **4789**.
- **flooding-type**
  Specifies the flooding type to use to transmit multicast, broadcast and unknown destination frames. The default is **multicast**.
- **regex**
  Displays the items that match the regular expression. The regular expression must be preceded by an at sign (@[regular expression]) to indicate that the identifier is a regular expression. See **help regex** for a description of regular expression syntax.

See Also

create, *delete*, *edit*, glob, *list*, *modify*, *tunnel*, regex, *show*, *tmsh*

wccp

Configures a Web-cache coordination protocol (WCCP) GRE profile.

Syntax

Configure the **wccp** component within the **net tunnels** module using the syntax in the following sections.

Create/Modify

```
create wccp [name]
modify wccp [name]
    app-service [[string] | none]
    defaults-from [name]
    description [string]
    rx-csum [disabled | enabled]
    tx-csum [disabled | enabled]
    wccp-version [1 | 2]
edit wccp [ [ [name] | [glob] | [regex] ] ... ]
      all-properties
      non-default-properties
```

Display

```
list wccp
list wccp [ [ [name] | [glob] | [regex] ] ... ]
show running-config wccp
show running-config wccp [ [ [name] | [glob] | [regex] ] ... ]
    all-properties
    app-service
    non-default-properties
    one-line
    partition
```

Delete

```
delete wccp [ all | [name] ]
```

Description

You can use the **wccp** component to create a WCCP GRE profile that you associate with a tunnel using the **tunnel** component. For more information about creating a tunnel see **net tunnel**.

Examples

create wccp my_wccp_gre

Creates a WCCP GRE profile called **my_wccp_gre**.

list wccp all-properties

Displays all of the properties of all of the WCCP GRE profiles.

Options

- **app-service**
  Specifies the name of the application service to which the object belongs. The default value is **none**. **Note:** If the **strict-updates** option is **enabled** on the application service that owns the object, you cannot modify or delete the object. Only the application service can modify or delete the object.
- **defaults-from**
  Specifies the existing profile from which the system imports settings for the new profile. The default value is **wccpgre**.
- **description**
  User defined description.
- **glob**
  Displays the items that match the **glob** expression. See **help glob** for a description of **glob** expression syntax.
- **name**
  Specifies a unique name for the component. This option is required for the commands **create** and **modify**.
- **partition**
  Displays the administrative partition within which the component resides.
- **regex**
  Displays the items that match the regular expression. The regular expression must be preceded by an at sign (@[regular expression]) to indicate that the identifier is a regular expression. See **help regex** for a description of regular expression syntax.
- **rx-csum**
  Specifies whether the system verifies the checksum on received packets. The default value is **disabled**.
- **tx-csum**
  Specifies whether the system includes a checksum on transmitted packets. The default value is **disabled**.
- **wccp-version**
  Specifies the version of WCCP that the system uses. The default value is **2**.

See Also

create, *delete*, *edit*, glob, *list*, *modify*, *gre*, *ipip*, *tunnel*, regex, *show*, *tmsh*

75

pem

- Introducing the PEM module
- Alphabetical list of components

Introducing the PEM module

You can use the tmsh components that reside within the Policy Enforcement Manager (pem) module to configure policy enforcement for the BIG-IP® system. For more information about the tmsh hierarchical structure, see Chapter 2, *Understanding and Using the Traffic Management Shell*.

Alphabetical list of components

The remainder of this chapter lists the tmsh components that are available in the pem module.

forwarding-endpoint

Configures forwarding endpoints for the Policy Enforcement Manager (PEM).

Syntax

Modify the **forwarding-endpoint** component within the **pem** module using the syntax shown in the following sections.

Create/Modify

```
create forwarding-endpoint [name]
modify forwarding-endpoint [name]
    app-service [[string] | none]
    persistence [destination-ip | disabled | source-ip]
    pool [name]
    snat-pool [name]
    source-port [change | preserve | preserve-strict]
    translate-address [enabled | disabled ]
    translate-service [enabled | disabled ]
edit forwarding-endpoint [ [ [name] | [glob] | [regex] ] ... ]
    all-properties
    non-default-properties
```

Display

```
list forwarding-endpoint
list forwarding-endpoint [ [ [name] | [glob] | [regex] ] ... ]
show running-config forwarding-endpoint
show running-config forwarding-endpoint [ [ [name] | [glob] | [regex] ] ... ]
    all-properties
    non-default-properties
    one-line
    partition
```

Delete

```
delete forwarding-endpoint [name]
```

◆ Note

All references to the forwarding-endpoint must be removed before it can be deleted.

Description

forwarding-endpoint is used to specify PEM policy forwarding action(s).

◆ Note

*A valid LTM pool with at least one member must be pre-configured before creating a forwarding-endpoint. Please refer to **ltm pool** for more info about configuring LTM pools.*

Examples

create forwarding-endpoint my_endpoint { pool my_pool snatpool my_snatpool source-port preserved translate-address enabled translate-service enabled }

Creates a Policy Enforcement Manager forwarding endpoint named **my_endpoint**.

delete forwarding-endpoint my_endpoint

Deletes the forwarding-endpoint named **my_endpoint**.

list forwarding-endpoint my_endpoint

Displays the properties of the forwarding-endpoint named **my_endpoint**.

Options

- **app-service**
  Specifies the name of the application service to which the object belongs. The default value is **none**. **Note:** If the **strict-updates** option is **enabled** on the application service that owns the object, user cannot modify or delete the object. Only the application service can modify or delete the object.
- **description**
  Specifies a user-defined description.
- **persistence**
  Allows to select an IP address to have the specific traffic to be forwarded to the same pool member.
  The options are:
  - **destination-ip**
    Map the destination ip address to a specific pool member so that subsequent traffic sent to this address is directed to the same pool member.
  - **source-ip**
    Map the source ip address to a specific pool member so that subsequent traffic from this address is directed to the same pool member.
  - **disabled**
    Specifies that this feature is disabled.

- **pool**
  Specifies the name of an LTM pool where the traffic is going to be directed to. Is used in the PEM policy rule forwarding actions. Note that the pool must be pre-configured before it can be referenced by a forwarding action.
- **snat-pool**
  Specifies the name of an existing LTM SNAT pool (snatpool) that is used to translate the client IP address to one of the configured IP addresses in that SNAT pool. The Self-IP addresses of the BIG-IP system must not be included in the SNAT pool. The default value is **none**.
- **source-port**
  Specifies whether the system preserves the source port of the connection. The default value is **preserve**.
  The options are:
  - **change**
    Specifies that the system changes the source port. This setting is useful for obfuscating internal network address.
  - **preserve**
    Specifies that the system preserves the value configured for the source port, unless the source port from a particular snat is already in use, in which case the system uses a different port.
  - **preserve-strict**
    Specifies that the system preserves the value configured for the source port. If the port is in use, the system does not process the connection. F5 Networks recommends restricting the use of this setting to cases that meet at least one of the following conditions:

The port is configured for UDP traffic.

The system is configured for nPath routing or is running in transparent mode (that is, there is no translation of any other Layer 3 or Layer 4 field).

There is a one-to-one relationship between virtual IP addresses and node addresses, or clustered multiprocessing (CMP) is disabled.

- **translate-address**
  Specifies, when enabled, that the system translates the original destination address of the virtual server. When disabled, specifies that the system uses the address without translation. The default value is **disabled**.
- **translate-service**
  Note that **translate-service** is really **translate-port**. It specifies, when enabled, that the system translates the original destination port. When disabled, it specifies that the system uses the original destination port without translation. The default value is **disabled**.

See Also

create, *delete*, *edit*, glob, *list*, *modify*, *interception-endpoint*, *listener*, *policy*, *diameter-endpoint*, *spm*, *format-script*, *service-chain-endpoint*, *subscriber*, *subscribers*, regex, *show*, *tmsh*

interception-endpoint

Configures interception endpoints for the Policy Enforcement Manager (PEM).

Syntax

Modify the **interception-endpoint** component within the **pem** module using the syntax shown in the following sections.

Create/Modify

```
create interception-endpoint [name]
modify interception-endpoint [name]
    app-service [[string] | none]
    persistence [destination-ip | disabled | source-ip]
    pool [name]
edit interception-endpoint [ [ [name] | [glob] | [regex] ] ... ]
    all-properties
    non-default-properties
```

Display

```
list interception-endpoint
list interception-endpoint [ [ [name] | [glob] | [regex] ] ... ]
show running-config interception-endpoint
show running-config interception-endpoint [ [ [name] | [glob] | [regex] ] ... ]
    all-properties
    non-default-properties
    one-line
    partition
```

Delete

```
delete interception-endpoint [name]
```

◆ Note

You must remove all references to an interception-endpoint before you can delete the interception-endpoint.

Description

You can use the **interception-endpoint** component to configure interception-endpoint definitions for the Policy Enforcement Manager. The interception-endpoint is used to clone all traffic. **Note:** Before you create a cloning-endpoint you have to create a valid pool. Please refer to **ltm pool** for more information about how to create a pool.

Examples

create interception-endpoint my_endpoint { pool pool1 }

Creates a Policy Enforcement Manager interception-endpoint named **my_endpoint**.

delete interception-endpoint my_endpoint

Deletes the interception-endpoint named **my_endpoint**.

list interception-endpoint my_endpoint

Displays the properties of the interception-endpoint named **my_endpoint**.

Options

- **app-service**
  Specifies the name of the application service to which the object belongs. The default value is **none**. **Note:** If the **strict-updates** option is **enabled** on the application service that owns the object, you cannot modify or delete the object. Only the application service can modify or delete the object.
- **persistence**
  Specifies the persistence that is based on either the source or destination IP addresses only.
- **pool**
  Specifies the pool. It is mandatory to specify a pool when creating any interception-endpoint. Before you create an interception-endpoint you have to create a valid **pool**.

See Also

create, *delete*, *edit*, glob, *list*, *modify*, *forwarding-endpoint*, *listener*, *policy*, *diameter-endpoint*, *spm*, *format-script*, *service-chain-endpoint*, *subscriber*, *subscribers*, regex, *show*, *tmsh*

irule

Configures an PEM iRule for traffic management system configuration.

Syntax

Configure the **irule** component within the **pem** module using the syntax shown in the following sections.

Create/Modify

```
create irule [name]
edit irule [name]
modify irule [ [ [name] | [glob] | [regex] ] ... ]
```

◆ Note

*When using tmsh, you can only create pem iRule using the editor, which starts when you use the create or edit commands. You cannot create an pem iRule directly on the command line. The vim editor applies the autoindent and smartindent options. You can toggle on/off paste mode using the **F12** key.*

◆ Note

You can also edit user metadata associated with a pem iRule. See the example section for more information.

Display

```
list irule
list irule [ [ [name] | [glob] | [regex] ] ... ]
show running-config irule
show running-config irule [ [ [name] | [glob] | [regex] ] ... ]
    all-properties
    non-default-properties
show irule
show irule [ [ [name] | [glob] | [regex] ] ... ]
    (default | exa | gig | kil | meg | peta | raw | tera | yotta | zetta)
    field-fmt
```

Delete

```
delete irule [name]
```

Description

You can apply **pem iRules** as an action when the traffic matches the filter criteria defined in **pem policy rule**. The syntax that you use to write pem iRules is based on the Tools Command Language (Tcl) programming

standard. Thus, you can use many of the stand Tcl commands, plus a robust set of extensions that the BIG-IP® policy enforcement management system provides to help you customize the actions you want to apply to the traffic.

You cannot edit the system iRules that come with the BIG-IP system. However, you can open a system iRule in the editor and use it as a template to create a new rule.

To create a new **pem iRule** using a system rule as a template:

1. Enter the command sequence **edit irule [system rule name]**.
   tmsh opens the system rule in an editor.
2. Change the name of the rule in the editor.
3. Edit the rule and exit the editor.
   tmsh checks for syntax errors, and if there are none, it saves the new rule.

For more information about iRules®, see **http://devcentral.f5.com/**.

Examples

list irule

Displays all iRules.

delete irule my_irule

Deletes the pem iRule named **my_irule**.

```
irule my_irule {
    priority 1
    when PEM_POLICY {
    }
}
```

Creates a pem iRule named **my_irule** with priority 1.

Modifies an existing pem iRule named **my_irule** by adding a new metadata and modifying an existing metadata:

```
modify rule my_irule {
    when RULE_INIT {}
    metadata replace-all-with {
        my_meta {
            persist false
            value "hello"
        }
        my_meta2 {
            persist false
            value "hello 2"
        }
    }
}
```

The metadata attribute is the user defined key/value pair. Metadata has the following format:

```
metadata
    [add | delete | modify] {
        [metadata_name] {
```

```
            value [ "value content" ]
            persist [ true | false ]
        }
    }
```

Deletes a metadata from a pem iRule:

```
modify irule my_irule {
    when RULE_INIT {}
    metadata delete { my_meta }
}
```

Options

- **glob**
  Displays the items that match the **glob** expression. See **help glob** for a description of **glob** expression syntax.
- **name**
  Specifies a unique name for the component. This option is required for the **create**, **delete**, and **modify** commands.
- **regex**
  Displays the items that match the regular expression. The regular expression must be preceded by an at sign (@[regular expression]) to indicate that the identifier is a regular expression. See **help regex** for a description of regular expression syntax.
- **meta-data**
  Specifies the user-defined key/value pair associated with the rule. See the example section for usage format.

See Also

create, *delete*, *edit*, glob, *list*, *modify*, regex, *show*, *tmsh*

listener

Configures listeners for the Policy Enforcement Manager (PEM).

Syntax

Modify the **listener** component within the **pem** module using the syntax shown in the following sections.

Create/Modify

```
create listener [name]
modify listener [name]
    app-service [[string] | none]
    description [string]
    profile-spm [name]
    virtual-servers [name] [add | delete | replace-all-with] {
       [virtual_server_name ... ]
    }
edit listener [ [ [name] | [glob] | [regex] ] ... ]
    all-properties
    non-default-properties
```

Display

```
list listener
list listener [ [ [name] | [glob] | [regex] ] ... ]
show running-config listener
show running-config listener [ [ [name] | [glob] | [regex] ] ... ]
    all-properties
    non-default-properties
    one-line
    partition
```

Delete

```
delete listener [name]
```

◆ Note

You must remove all references to a listener before you can delete the listener.

Description

You can use the **listener** component to configure listener definitions for the Policy Enforcement Manager.

Examples

create listener lis1 { profile-spm spm1 virtual-servers add {vs_tcp vs_udp} }

Creates a Policy Enforcement Manager listener named **lis1**.

delete listener lis1

Deletes the listener named **lis1**.

list listener lis1

Displays the properties of the listener named **lis1**.

Options

- **app-service**
  Specifies the name of the application service to which the object belongs. The default value is **none**. **Note:** If the **strict-updates** option is **enabled** on the application service that owns the object, you cannot modify or delete the object. Only the application service can modify or delete the object.
- **description**
  User defined description.
- **profile-spm**
  Specifies the spm profile name.
- **virtual-servers**
  Adds, deletes, or replaces a set of virtual servers, by specifying a virtual server name.

See Also

create, *delete*, *edit*, glob, *list*, *modify*, *forwarding-endpoint*, *interception-endpoint*, *policy*, *diameter-endpoint*, *spm*, *format-script*, *service-chain-endpoint*, *subscriber*, *subscribers*, regex, *show*, *tmsh*

policy

Configures policies for the Policy Enforcement Manager (PEM).

Syntax

Modify the **policy** component within the **pem** module using the syntax shown in the following sections.

Create/Modify

```
create policy [name]
modify policy [name]
  description [string]
  status [enabled | disabled]
  transactional [enabled | disabled]
  rules [add | delete | modify | replace-all-with] {
     [rule_name ... ] {
        app-service [[string] | none]
        classification-filters [add | delete | modify | replace-all-with] {
           [filter_name ...] {
              app-service [[string] | none]
              application [application_name]
              category [category_name]
              operation [match | nomatch]
           }
        }
        dscp-marking-downlink [integer]
        dscp-marking-uplink [integer]
        flow-info-filters [add | delete | modify | replace-all-with] {
           [filter-name ...] {
              app-service [[string] | none]
              dscp-code [integer]
              dst-ip-addr [ip address/prefixlen]
              dst-port [port]
              from-vlan [vlan_name]
              l2-endpoint [disabled | vlan]
              operation [match | nomatch]
              ip-addr-type [IPv4 | IPv6 | any]
              proto [ tcp | udp | any]
              src-ip-addr [ip address/prefixlen]
              src-port [port]
           }
        }
        flow-info-filters [none]
        forwarding {
            endpoint [forwarding_endpoint_name]
            fallback-action [drop | continue]
            internal-virtual [name]
            icap-type [request | response | both | none]
            type [icap | pool | route-to-network | none]
        }
        gate-status [enabled | disabled]
        http-redirect {
            redirect-url [string]
            fallback-action [drop | continue]
        }
```

```
        intercept [intercept_endpoint_name]
        l2-marking-downlink [integer]
        l2-marking-uplink [integer]
        modify-http-hdr {
            name [header_name]
            operation [insert | none | remove]
            value-content [header_value]
            value-type [string | tcl-snippet]
        }
        precedence [integer]
        reporting {
            dest {
               gx {
                   endpoint-id [name]
               }
               hsl {
                   endpoint-id [ name]
                   format-script [name]
                   session-reporting-fields
                      [add | delete | replace-all-with] {
                        [reporting field ... ]
                   }
                   flow-reporting-fields
                      [add | delete | replace-all-with] {
                        [reporting field ... ]
                   }
                   transaction_reporting_fields
                      [add | delete | replace-all-with] {
                        [reporting field ... ]
                   }
               }
               radius-accounting {
                   radius-aaa-virtual [name]
               }
            }
            granularity [flow | session | transaction]
            interval [integer]
            transaction {
               http {
                   hostname-len [integer]
                   uri-len [integer]
                   user-agent-len [integer]
               }
            }
            volume {
                downlink
                total
                uplink
            }
        }
    quota {
            rating-group [name]
            reporting-level [rating-group | service-id]
        }
        qos-rate-pir-downlink [bwc policy name | none]-> [category name | none]
        qos-rate-pir-uplink [bwc policy name | none]-> [category name | none]
        service-chain [service chain endpoint name]
        tcl-filter [tcl-script]
        url-categorization-filters [add | delete | modify | replace-all-with] {
           [filter_name ...] {
              category [category_name]
              operation [match | nomatch]
```

```
            }
          }
        }
      }
      rules [none]
edit policy [ [ [name] | [glob] | [regex] ] ... ]
    all-properties
    non-default-properties
```

Display

```
list policy
list policy [ [ [name] | [glob] | [regex] ] ... ]
show running-config policy
show running-config policy [ [ [name] | [glob] | [regex] ] ... ]
  all-properties
  non-default-properties
  one-line
  partition
show policy
show policy [name]
  all-properties
  (default | exa | gig | kil | meg | peta | raw | tera | yotta | zetta)
  detail
  field-fmt
```

Delete

```
delete policy [name]
```

◆ Note

You must remove all references to a policy before you can delete the policy.

Description

You can use this **policy** component to configure the policy definitions on the Policy Enforcement Manager. A policy is a set of rules which are used to match traffic flow and apply actions. A rule has configuration for filters and actions. All configured filters must match before the actions can be applied to the traffic flow. There are four filters: classification-filter, url-category-filter, flow-info-filter, and tcl-filter. Classification-filter allows for matching the traffic based on the flow L7 features, such as a specific application (for example, Google Mail) or application category (for example, Web). URL-category-filter allows for mathing the type of URL, such as adult content. Flow-info-filter allows for matching the traffic using L2-L4 flow parameters. Tcl-filter provides a customized method to match traffic flows using iRule commands. The actions can be steering or/and reporting. Steering allows the user to manipulate the traffic when all configured filters match the flow. The steering options can be forwarded (option **forwarding**), drop/pass(option **gate-status**), redirect(option **http-redirect**), or intercept(option **intercept**). Reporting allows the user to report the usage to different endpoints by different output formats. The

reporting options can be gx or hsl. Policy attribute **transactional** allow policy enforcement for HTTP traffic for each transaction. Quota allows users to do quota management over Gy by specifying the rating group, which has all the parameters associated.

Examples

```
create policy my_policy rules add {
   rule_1 {
      flow-info-filters {
         flow_1 {
            dscp-code 8
         }
         flow_2 {
            dst-port 80
         }
         forwarding {
            endpoint server1
            fallback-action continue
         }
      }
      precedence 1
   }
   rule_2 {
      reporting {
         dest {
            hsl {
               endpoint-id pem_hsl
               format-script fm1
            }
         }
         granularity flow
         volume {
            total 5000
         }
      }
      precedence 2
   }
 }
```

Creates a Policy Enforcement Manager policy named **my_policy** with two rules, **rule_1** and **rule_2**. **rule_1** defines the flow-info-filters so that when the flow with DSCP is 8 or destination port is 80, the traffic will be forwarded to server1. **rule_2** defines a flow-based reporting rule which will send flow usage record to pem_hsl endpoint using format script defined in fm1 whenever total increases by 5000 bytes.

delete policy my_policy

Deletes the policy named **my_policy**.

list policy my_policy

Displays properties of the policy named **my_policy**.

Options

- **app-service**
  Specifies the name of the application service to which the policy belongs. The default value is **none**. **Note:** If the **strict-updates** option is **enabled** on the application service that owns the object, you cannot modify or delete the policy. Only the application service can modify or delete the policy.
- **description**
  User defined description.
- **transactional**
  Indicate the policy enable or disable policy enforcement for each HTTP transaction.
- **partition**
  Displays the administrative partition within which the policy resides.
- **rules**
  Adds, deletes, or replaces a set of rules, by specifying a rule name. If a rule by the specified name does not exist, it will be created. You can configure the following options for a rule:
  - **app-service**
    Specifies the name of the application service to which the rule belongs. The default value is **none**. **Note:** If the **strict-updates** option is **enabled** on the application service that owns the object, you cannot modify or delete the rule. Only the application service can modify or delete the rule.
  - **classification-filters**
    Adds, deletes, or replaces a set of classification-filters. You can configure the following options for a classification-filter.
    - **app-service**
      Specifies the name of the application service to which the classification-filter belongs. The default value is **none**. **Note:** If the **strict-updates** option is **enabled** on the application service that owns the object, you cannot modify or delete the rule. Only the application service can modify or delete the classification-filter.
    - **application**
      Specifies the name of the application where the rule applies to the traffic. The default value is **none**.
    - **category**
      Specifies the name of the category of applications where the rule applies to the traffic. The default value is **none**.
    - **operation**
      The options **match** and **nomatch** indicate the traffic flow must match or not match the condition specified in the classification filter. The default value is **match**.

- **dscp-marking-downlink**
  Specifies the action to modify the DSCP code in the downlink packet when the traffic flow matches the rule matching criteria. The range is **0** to **63**, or **pass-through**. The default value is **pass-through**, indicating the DSCP code of the downlink packet will not be changed when the traffic flow matches the rule.
- **dscp-marking-uplink**
  Specifies the action to modify the DSCP code in the uplink packet when the traffic flow matches the rule matching criteria. The range is **0** to **63**, or **pass-through**. The default value is **pass-through**, indicating the DSCP code of the uplink packet will not be changed when the traffic flow matches the rule.
- **flow-info-filters**
  Adds, deletes, or replaces a set of the flow-info-filters. The flow info filter defines the flow conditions (Layer 4) that the traffic should meet (or not meet) for this enforcement policy rule to apply. You can configure the following options for a flow-info-filter.
  - **app-service**
    Specifies the name of the application service to which the flow-info-filter belongs. The default value is **none**. **Note:** If the **strict-updates** option is **enabled** on the application service that owns the object, you cannot modify or delete the rule. Only the application service can modify or delete the flow-info-filter.
  - **dscp-code**
    Specifies the value of DSCP code which matches incoming traffic based on a value in the DSCP field in the IP header. The range is **0** to **63**, or **disabled**. The default value is **disabled**, indicating that the DSCP code will not be used to filter the packet in the flow-info-filter.
  - **dst-ip-addr**
    Specifies the destination IP address and prefix length that the rule applies to. The format is [ip address/prefixlen]. The default value is **0.0.0.0/0**.
  - **dst-port**
    Specifies the destination port against which the packet will be compared. The default value is **any**.
  - **from-vlan**
    Specifies the name of the source vlan to match the ingress flow arriving from that vlan.
  - **l2-endpoint**
    Specifies an L2 endpoint type to be used when matching the traffic flows. The default value is **disabled**, indicating that L2 endpoint is not used for matching the flows. You can configure the following options:
  - **disabled**
    Flows are not matched based on the L2 endpoint specification.

- **vlan**
  The vlan name specified in **from-vlan** is used to match the traffic flows.
- **operation**
  Specifies whether the rule applies to traffic that matches (**match**) or does not match (**nomatch**) the traffic flow defined here. The options are **match** and **nomatch**. The default value is **match**.
- **proto**
  Specifies the protocol that this rule applies to. The options are **any**, **tcp**, and **udp**. The default value is **any**.
- **ip-add-type**
  Specifies the ip address type (IPv4 or IPv6) that this rule applies to. The options are **any**, **IPv4**, and **IPv6**. The default value is **any**.
- **src-ip-addr**
  Species the source IP address and prefix length that the rule applies to. The format is [ip address/prefixlen]. The default value is **0.0.0.0/0**.
- **src-port**
  Specifies the source port of the network you want the rule to affect. The default value is **any**.

- **forwarding**
  Manages the forwarding action and its attributes.
  - **endpoint**
    Specifies the forwarding endpoint. The endpoint can be icap, pool or route-to-network. Depending on the type chosen flow can be steered to icap server, pool or to the network.
  - **fallback-action**
    Specifies whether the connection should continue unchanged or should be dropped in the event the forwarding action fails for any reason. The options are: drop or continue, and the default is **drop**.
  - **internal-virtual**
    Specifies the internal virtual server name if the type selected is icap.
  - **icap-type**
    Defines the ICAP adaptation type: request only adaptation, request and response adaptation or both types of adaptations combined.
  - **type**
    Specifies the type of forwarding action.
- **gate-status**
  Specifies, when set to **enabled**, that the traffic can pass through the system without being changed. Set **disabled** to drop traffic that this rule applies to. The options are **disabled** and **enabled**. The default is **enabled**.
- **http-redirect**
  Manages the HTTP redirect action and its attributes.
  - **redirect-url**
    Specifies the HTTP redirection URL.

- **fallback-action**
  Specifies whether the connection should continue unchanged or should be dropped in the event the forwarding action fails for any reason. The options are: drop or continue, and the default is **drop**.
- **intercept**
  Specifies the name of the intercept endpoint.
- **l2-marking-downlink**
  Set Layer-2 Quality of Service Marking in downlink traffic that matches a rule. Setting a L2 QoS Marking affects the packet delivery priority. The range is **0** to **7**, or **pass-through**. The default value is **pass-through**, indicating the L2 QoS Marking of the packet will not be changed when the packet matches the rule.
- **l2-marking-uplink**
  Set Layer-2 Quality of Service Marking in uplink traffic that matches a rule. Setting a L2 QoS marking affects the packet delivery priority. The range is **0** to **7**, or **pass-through**. The default value is **pass-through**, indicating the L2 QoS Marking of the packet will not be changed when the packet matches the rule.
- **modify-http-hdr**
  Specifies the action to modify the HTTP header when the traffic flow matches the rule matching criteria. You can configure the following options for modifying the HTTP header.
- **name**
  Specifies the HTTP header name used by the **operation** option to modify the HTTP header.
- **operation**
  Specifies the operation used to modify the HTTP header. The options are **insert**, **none**, and **remove**. The default value is **none** which indicates that no HTTP header modifications will be made.
- **value-content**
  Specifies the HTTP header value content used by the **operation** option to modify the HTTP header. Based on the selected **value-type** option, the content format will be interpreted either as a string or a tcl snippet. Note: This field is applicable only when the **operation** option is set to **insert**.
- **value-type**
  Specifies the type of content format used in the **value-content** field. The options are **string** and **tcl-snippet**. The default value is **string** which indicates that the **value-content** field will be interpreted as a string.
- **precedence**
  Specifies the precedence for the rule in relation to the other rules. The range is **1** to **4294967295** where **1** has the highest precedence. A rule with higher precedence is evaludated at a high priority. It is mandatory to specify precedence when creating a rule in a policy.
- **reporting**
  You can configure the following options for reporting.

- **dest**
  You can configure the following options for destination.
- **gx**
  You can configure the following options for gx endpoint.
- **endpoint-id**
  Specifies the endpoint name.
- **hsl**
  You can configure the following options for hsl endpoint.
- **endpoint-id**
  Specifies the endpoint name.
- **format-script**
  Specifies the format script name to format the HSL output string format.
- **session-reporting-fields**
  Specifies the session fields and their order based on which messages should be published.
- **flow-reporting-fields**
  Specifies the flow fields and their order based on which messages should be published.
- **transaction-reporting-fields**
  Specifies the transaction fields and their order based on which messages should be published.
- **radius-accounting**
  You can configure the following options for radius-accounting endpoint.
- **radius-aaa-virtual**
  Specifies the internal virtual server for radius-accounting endpoint.
- **granularity**
  Specifies the type of reporting will be generated when the policy applies. The options are **flow**, **session** and **transaction**. The default value is **session** which indicates the session report will be generated if this policy applies.
- **interval**
  Specifies the time interval in seconds the report will be generated. The default value is **0** which indicates this feature is disabled.
- **transaction**
  You can configure the following options when the **transaction** report granularity is selected.
- **http**
  Specifies the HTTP transaction report options for the following HTTP attributes.
- **hostname-len**
  Specifies the maximum HTTP hostname string length to include in the HTTP transaction report. The range is **0** to **65535**. The default value is **0**.

- **uri-len**
  Specifies the maximum HTTP URI string length to include in the HTTP transaction report. The range is **0** to **65535**. The default value is **256**.
- **user-agent-max**
  Specifies the maximum HTTP user agent string length to include in the HTTP transaction report. The range is **0** to **65535**. The default value is **0**.
- **volume**
  You can configure the following options for volume threshold. The report will be generated when any of the following conditions happened. If reporting dest is set, either **interval** must be set to non-0 or one of **volume** properties must be set to non-0.
- **downlink**
  The report will be generated if the downlink traffic exceeds the threshold. The default value is **0** which indicates this feature is disabled.
- **total**
  The report will be generated if the uplink and downlink traffic exceeds the threshold. The default value is **0** which indicates this feature is disabled.
- **uplink**
  The report will be generated if the uplink traffic exceeds the threshold. The default value is **0** which indicates this feature is disabled.
- **quota**
  You can configure the following options for quota management.
- **rating-group**
  Specifies the rating-group name.
- **reporting-level**
  Specifies the quota reporting level whether per rating group or per service-id.
- **qos-rate-pir-downlink**
  Specifies the configured bandwidth control policy for Peak Information Rate (PIR) to apply to downlink traffic that matches this rule. Use **none** to reset bwc policy name or category name.
- **qos-rate-pir-uplink**
  Specifies the configured bandwidth control policy for Peak Information Rate (PIR) to apply to uplink traffic that matches this rule. Use **none** to reset bwc policy name or category name.
- **service-chain**
  Specifies where to forward the traffic affected by this rule.
- **tcl-filter**
  Specifies the tcl expression which uses iRule commands to filter the packet. It is a match if tcl-filter returns TRUE/1 or nomatch if

FALSE/0. All configured filters (flow-info-filters, classification-filters, and tcl-filter) must match before rule actions are applied.

- **url-categorization-filters**
  Adds, deletes, or replaces a set of url-categorization-filters. You can configure the following options for a url-categorization-filter.
  - **app-service**
    Specifies the name of the application service to which the url-categorization-filter belongs. The default value is **none**. **Note:** If the **strict-updates** option is **enabled** on the application service that owns the object, you cannot modify or delete the rule. Only the application service can modify or delete the url-categorization-filter.
  - **url-category**
    Specifies the name of the url-category of the traffic where the rule applies. The default value is **none**.
  - **operation**
    The options **match** and **nomatch** indicate the traffic flow must match or not match the condition specified in the classification filter. The default value is **match**.
- **status**
  Specifies the current status of the policy. The options are **disabled** and **enabled**. The default value is **enabled**.

See Also

create, *delete*, *edit*, glob, *list*, *modify*, *forwarding-endpoint*, *interception-endpoint*, *listener*, *diameter-endpoint*, *spm*, *format-script*, *service-chain-endpoint*, *subscriber*, *subscribers*, regex, *reset-stats*, *show*, *tmsh*

service-chain-endpoint

Configures service chain endpoints for the Policy Enforcement Manager (PEM).

Syntax

Modify the **service-chain-endpoint** component within the **pem** module using the syntax shown in the following sections.

Create/Modify

```
create service-chain-endpoint [name]
modify service-chain-endpoint [name]
    app-service [[string] | none]
    service-endpoints [add | delete | modify | replace-all-with] {
        [service endpoint name ... ] {
                 app-service [[string] | none]
                 forwarding-endpoint
                     to-endpoint [forwarding endpoint name]
                 from-vlan [vlan name]
                 http-adapt-service
                     internal-virtual [internal virtual server | none]
                     icap-type [request | response | both | none]
                 order [integer]
                 service-option [optional | mandatory]
                 steering-policy [policy name | none]
        }
    }
edit service-chain-endpoint [ [ [name] | [glob] | [regex] ] ... ]
    all-properties
    non-default-properties
```

Display

```
list service-chain-endpoint
list service-chain-endpoint [ [ [name] | [glob] | [regex] ] ... ]
show running-config service-chain-endpoint
show running-config service-chain-endpoint [ [ [name] | [glob] | [regex] ] ... ]
    all-properties
    non-default-properties
    one-line
    partition
```

Delete

```
delete service-chain-endpoint [name]
```

◆ Note

You must remove all references to a service-chain-endpoint before you can delete the service-chain-endpoint.

Description

You can use the **service-chain-endpoint** component to configure service-chain-endpoint definitions for the Policy Enforcement Manager (PEM). Each service-chain-endpoint consists of one or more service-endpoints, where a service-endpoint consists of a non-zero integer order, existing **from-vlan** a valid fwd-endpoint or a http-adapatation-service endpoint. When you configure a BIG-IP that has a service-chain-endpoint with multiple service-endpoints, traffic will pass through different endpoints choosen dynamically.

◆ Note

*You must create a valid forwarding-endpoint and a valid vlan before you can create a service-endpoint. If you are enabling **http-adapt-service**, you must create Request Adapt and Response Adapt profiles and attach to the traffic virtual. Also create an **internal-virtual** and enable icap profile. You must also give each service-endpoint an order from 1 up to 2^32-1. The lower the service-endpoint order is, the higher its precedence is (i.e., traffic will pass though it before other higher order service-endpoints). Each service-endpoint has a boolean (true/false) **service-option** that defines what would happen if the service-endpoint is down. If **service-option** is mandatory, the traffic flow is dropped if the service-endpoint is down. If **service-option** is optional, the traffic flow will be bypassed to the next available service-endpoint.*

For more information about how to create a vlan, please refer to **net vlan**. Also please refer to **pem forwarding-endpoint** for more information about how to create a **pem forwarding-endpoint**.

Examples

create service-chain-endpoint chain1 service-endpoints add { ser_ep1 { order 10 from-vlan vlan1 forwarding-endpoint { to-endpoint fw_ep1 } service-option optional } ser_ep2 { order 5 from-vlan vlan2 http-adapt-service {internal-virtual iv1} service-option mandatory } }

Creates a PEM service-chain-endpoint named **chain1** that has two service-endpoints: ser_ep1 and ser_ep2. The first ser_ep1 has an order of 10 and is optional and has **forwarding-endpoint** with **to-endpoint** fw_ep1, type transparent and vlan1 as a **from-vlan**. The second ser_ep2 has an order of 5 is mandatory and has **http-adapt-service** enabled with ivs1 as **internal-server** and vlan2 as a **from-vlan**. Note that **ser_ep2** will precede **ser_ep1** because the lower the service-endpoint order is, the higher its precedence is.

delete service-chain-endpoint chain1

Deletes the service-chain-endpoint named **chain1**.

list service-chain-endpoint chain1

Displays the properties of the service-chain-endpoint named **chain1**.

Options

- **app-service**
  Specifies the name of the application service to which the object belongs. The default value is **none**. **Note:** If the **strict-updates** option is **enabled** on the application service that owns the object, you cannot modify or delete the object. Only the application service can modify or delete the object.
- **service-endpoints**
  Adds, deletes, or replaces a set of the service endpoints by specifying a series of service-endpoint names. If any of these names did not exist before, then new names will be created. Each service-endpoint is identified by a vlan and a forwarding-endpoint.
  - **app-service**
    Specifies the name of the application service to which the object belongs. The default value is **none**. **Note:** If the **strict-updates** option is **enabled** on the application service that owns the object, you cannot modify or delete the object. Only the application service can modify or delete the object.
  - **forwarding-endpoint**
    Specifies the forwarding endpoint attributes to be set. The below attributes can be set:
    - **to-endpoint**
      This is a default endpoint that will be chosen if steering policy is not configured. You have to create a valid PEM **forwarding-endpoint** before you can add **to-endpoint** to a **service-endpoint**.
  - **from-vlan**
    Specifies the vlan that the traffic will come from toward the service-endpoint. **Note:** The vlan has to exist before you can create a **from-vlan** field.
  - **http-adapt-service**
    Specifies the option to set attributes for http adapt services. Below are the attributes that can be set.
    - **internal-virtual**
      This is the internal virtual on which icap is enabled. You have to create the internal-virtual and assign icap profile before adding here.
    - **icap-type**
      Defines the ICAP adaptation type: request only adaptation, request and response adaptation or both types of adaptations combined.
  - **order**
    Specifies the order of the service-endpoint among other service-endpoints. The lower the service-endpoint's order is, the more precedence it has (i.e., the traffic will go through the lowest-ordered service-endpoint first, then through higher order service-endpoint, ... etc.).

- **service-option**
  Specifies the behavior when a service-endpoint is not available (i.e., is down). This option is limited when ICAP is defined as the service-endpoint and will not apply if the ICAP service is unavailable. You can configure the following options:
  - **mandatory**
    If the service-endpoint is down, the traffic flow is dropped.
  - **optional**
    If the service-endpoint is down, the traffic flow will be bypassed to the next available service-endpoint.
- **steering-policy**
  If the steering policy is configured, the policy is evaluated and if steering is enabled the flow will be steered to the corresponding endpoint.

See Also

create, *delete*, *edit*, glob, *list*, *modify*, *forwarding-endpoint*, *interception-endpoint*, *listener*, *policy*, *diameter-endpoint*, *spm*, *format-script*, *subscriber*, *subscribers*, regex, *show*, *tmsh*

sessiondb

Displays, deletes, modifies, and reset-stats a PEM subscriber session record on the BIG-IP® system.

Syntax

Use the **sessiondb** component within the **pem** module to view, delete, modify or reset statistics on a session record using the following syntax.

Note: Delete and Modify commands apply to all IP addresses if there are multiple IP addresses in a session.

Display

```
show sessiondb subscriber-id [string]
show sessiondb session-ip [ip address]
    all-properties
```

Delete

```
delete sessiondb
    subscriber-id [string]
    session-ip [ip address]
```

Modify

```
modify sessiondb
    subscriber-id [string]
    session-ip [ip address]
    session-state [marked-for-deletion | not-provisioned | provisioned |
provisioning-pending ]
```

Reset-Stats

```
reset-stats sessiondb
    subscriber-id [string]
    session-ip [ip address]
```

Description

You can use the **sessiondb** component to display session record in the sessionDB on the BIG-IP system. Additionally, you can delete, reset-stats and modify a specified session record from the sessionDB. Either

subscriber-id or **session-ip** must be specified as the query key to sessionDB. **session-state** must be specified in modify command. Wildcard query is not supported.

◆ Note

*show and reset-stats commands apply to both static and dynamic subscribers. delete and modify command only apply to dynamic subscribers. The session of static subscribers cannot be deleted. The session-state of static subscribers cannot be changed. To delete a static subscriber session you have to delete the static subscriber configuration in **pem subscriber**.*

Examples

show sessiondb subscriber-id 4085551212

Displays the session record of subscriber id 4085551212 in the sessionDB.

show sessiondb session-ip 10.10.10.100

Displays the session record of session ip address 10.10.10.100 in the sessionDB.

show sessiondb subscriber-id 4085551212 all-properties

Displays the session record of subscriber id 4085551212 in the sessionDB, and statistics for each IP.

show sessiondb session-ip 10.10.10.100 all-properties

Displays the session record of session ip address 10.10.10.100 in the sessionDB, and statistics for each IP.

delete sessiondb subscriber-id 4085551212

Deletes the session record of subscriber id 4085551212 from the sessionDB.

delete sessiondb session-ip 10.10.10.100

Deletes the session record of IP address 10.10.10.100 from the sessionDB.

reset-stats sessiondb subscriber-id 4085551212

Reset the session statistics of subscriber id 4085551212 from the sessionDB. **Flows Current** specifies the active flows and it cannot be reset.

modify sessiondb subscriber-id 4085551212 session-state provisioned

Modify the session state of subscriber id 4085551212 to **provisioned**.

Options

- **session-ip**
  Specifies the IP address of the subscriber session record. You can enter this address in either IPv4 or IPv6 format.
- **subscriber-id**
  Specifies the subscriber ID of the subscriber session record.

- **session-state**
  Specifies the subscriber session state of the subscriber session record that you want to modify. It is only required in modify command.
  The options are:
  - **marked-for-deletion**
    Specifies the subscriber session to be scheduled for deletion.
  - **provisioned**
    Specifies the subscriber session state to be marked as provisioned, regardless of whether the policies have been assigned or not. The unknown subscriber policies are not applied to the subscriber flows, even if no subscriber policies are provisioned.
  - **not-provisioned**
    Specifies the subscriber session state to be marked as not-provisioned. No further attempts to provision the session are made. The unknown subscriber policies are applied to the subscriber flows.
  - **provisioning-pending**
    Specifies the subscriber session state to be marked as having in process of provisioning. This will trigger a session provisioning request (e.g. Gy CCR request) immediately. If no response is received, or the provisioning process fails for any reason, another request will be sent after the retry timeout, until the session is provisioned successfully, or the number of retries is reached.

See Also

delete, *modify*, *reset-stats*, *show*, *tmsh*

subscriber

Configures subscribers for the Policy Enforcement Manager (PEM).

Syntax

Modify static **subscriber** component within **PEM** module using the syntax shown in the following sections.

Create/Modify

```
create subscriber [name]
modify subscriber [name]
    app-service [[string] | none]
    ip-address-list [add | delete | replace-all-with] {
       [ip address ...]
    }
    policies [add | delete | replace-all-with] {
       [policy_name ...]
    }
    policies [default | none]
    subscriber-id-type [dhcp | dhcp-custom | e164 | imsi | mac-address | mac-dhcp | nai
| private ]
edit subscriber [ [ [name] | [glob] | [regex] ] ... ]
    all-properties
    non-default-properties
```

Display

```
list subscriber
list subscriber [ [ [name] | [glob] | [regex] ] ... ]
show running-config subscriber
show running-config subscriber [ [ [name] | [glob] | [regex] ] ... ]
    all-properties
    non-default-properties
    one-line
    partition
```

Delete

```
delete subscriber [name]
```

◆ Note

You must remove all references to a subscriber before you can delete the subscriber.

Description

You can use the **subscriber** component to configure subscriber definitions for the Policy Enforcement Manager.

Examples

create subscriber 4085551212 { ip-address-list add { 10.10.10.2 10.10.10.3 } policies add { policy1 } subscriber-id-type imsi }

Creates a PEM subscriber **4085551212** with IP addresses **10.10.10.2** and **10.10.10.3**, subscriber id type **imsi**, and a policy **policy1**.

delete subscriber sub1

Deletes the subscriber named **sub1**.

list subscriber sub1

Displays the properties of the subscriber named **sub1**.

Options

- **app-service**
  Specifies the name of the application service to which the object belongs. The default value is **none**. **Note:** If the **strict-updates** option is **enabled** on the application service that owns the object, you cannot modify or delete the object. Only the application service can modify or delete the object.
- **name**
  Specifies a unique subscriber identifier (up to 64 characters). This option is required for the commands **create**, **delete**, and **modify**.
- **ip-address-list**
  Adds, deletes, or replaces a list of the ip address to associate with the subscriber.
- **policies**
  Adds, deletes, or replaces a set of the policies to associate with the subscriber.
- **subscriber-id-type**
  Specifies the format to use for the subscriber id. The default value is **imsi**.
  The options are:
  - **dhcp**
    For subscribers discovered via DHCP: an identifier comprises either Relay Option (option 82) for DHCPv4 based subscriber IDs or REMOTE-ID and SUBSCRIBER-ID Options (options 37 and 38) for DHCPv6, as configured in the corresponding DHCP profile.
  - **dhcp-custom**
    For subscribers discovered via DHCP: an identifier created using a custom TCL snippet.
  - **e164**
    A numbering plan that defines the format of an MSISDN international phone number (up to 15 digits). The number typically consists of three fields: country code, national destination code, and subscriber number.

- **imsi**
  International Mobile Subscriber Identity. A globally unique code number that identifies a GSM, UMTS, or LTE mobile phone user.
- **mac-address**
  For subscribers discovered via DHCP: subscriber MAC address in a standard IEEE 802 format for MAC-48 (six groups of two hexadecimal digits, separated by colons ':').
- **mac-dhcp**
  For subscribers discovered via DHCP: a concatenation of **mac-address** and **dhcp** identifier as configured in the corresponding DHCP profile.
- **nai**
  Network Access Identifier. A fully qualified network name in the form <user>@<realm>; identifies a subscriber and the home network to which the subscriber belongs.
- **private**
  The subscriber id type is private for the given deployment.

See Also

create, *delete*, *edit*, glob, *list*, *modify*, *forwarding-endpoint*, *interception-endpoint*, *listener*, *policy*, *diameter-endpoint*, *spm*, *format-script*, *service-chain-endpoint*, regex, *show*, *tmsh*

subscribers

Loads static subscribers for the Policy Enforcement Manager (PEM) from a file.

Syntax

Loads static subscribers from a file within the **pem** module using the syntax shown in the following sections.

Load

load subscribers file [filename]

Description

You can use the command **load pem subscribers** to load static subscribers definitions for the Policy Enforcement Manager (PEM). The maximum number of static subscribers allowed is (2 * sys db variable **tmm.pem.spm.maxsessionlimit**) or 100000, whichever is the lesser.

The static subscribers file is a csv file with the following fields: <Subscriber ID>,<Subscriber ID Type>,<Number of IP address>[,<IP address N>]*[,<Policy N>]+. Each record can have zero IP address but must have at least one policy.

The maximum number of IP addresses per subscriber is set by sys db variable **tmm.pem.session.ip.addr.max**.

The maximum number of IPv4 addresses per subscriber is set by sys db variable **tmm.pem.session.ipv4.addr.max**.

The maximum number of IPv6 addresses per subscriber is set by sys db variable **tmm.pem.session.ipv6.addr.max**.

For example, these are the examples from such file:

subscriber1,e164,2,11.1.1.1,11.1.1.2,bronze,gold,silver

subscriber2,imsi,0,gold

The filename either absolute file name or just the base file name under folder: /var/local/pem/subscribers/

For more information about static subscriber, please refer to **pem subscriber** module.

Examples

load subscribers file my_ss_file

Loads static subscribers from file "my_ss_file" under the folder: /var/local/pem/subscribers/.

load subscribers file /shared/tmp/new_ss_file

Loads static subscribers from file "new_ss_file" under the folder: /shared/tmp/.

See Also

create, *delete*, *edit*, glob, *list*, *modify*, *forwarding-endpoint*, *interception-endpoint*, *listener*, *policy*, *diameter-endpoint*, *spm*, *format-script*, *service-chain-endpoint*, regex, *show*, *tmsh*

76

pem global-settings

- Introducing the PEM global-settings module
- Alphabetical list of components

Introducing the PEM global-settings module

You can use the tmsh components that reside within the Policy Enforcement Manager (PEM) global-settings module to configure policy enforcement for the BIG-IP® system. For more information about the tmsh hierarchical structure, see Chapter 2, *Understanding and Using the Traffic Management Shell*.

Alphabetical list of components

The remainder of this chapter lists the tmsh components that are available in the pem global-settings module.

analytics

Configures the global settings that pertain to Analytics reporting for Policy Enforcement Manager (PEM).

Syntax

Modify the **analytics** component within the **pem global-settings** module using the syntax shown in the following sections.

Modify

```
modify analytics {
    mode [enable | disable]
    logging {
       hsl {
           endpoint-id [log-publisher]
       }
    }
}
edit analytics [ [ [name] | [glob] | [regex] ] ... ]
    all-properties
    non-default-properties
```

Display

```
list analytics
list analytics [ [ [name] | [glob] | [regex] ] ... ]
show running-config analytics
show running-config analytics [ [ [name] | [glob] | [regex] ] ... ]
    all-properties
    non-default-properties
    one-line
    partition
```

Description

You can use the **analytics** component to configure global settings for analytics reporting.

Examples

modify analytics mode disable logging hsl endpoint-id hsl_endpoint

Enables the analytics reporting for PEM and configures logging endpoint as hsl_endpoint.

list analytics

Displays the configuration for analytics settings.

Options

- **mode**
  Specifies the mode for analytics reporting. It can take enable or disable as value.
- **logging**
  You can configure the following option for logging.
  - **hsl**
    You can configure the following options for hsl endpoint.
    - **endpoint-id**
      Specifies the endpoint name.

See Also

create, *delete*, *edit*, glob, *list*, *modify*, *listener*, *policy*, *diameter-endpoint*, *spm*, *format-script*, *service-chain-endpoint*, *subscriber*, *subscribers*, regex, *show*, *tmsh*

quota-mgmt

Configures the global settings that pertain to quota management over Gy for Policy Enforcement Manager (PEM).

Syntax

Modify the **quota-mgmt** component within the **pem global-settings** module using the syntax shown in the following sections.

Modify

```
modify quota-mgmt
    default-rating-group [rating-group-name]
    service-context-id [string]
edit quota-mgmt [ [ [name] | [glob] | [regex] ] ... ]
    all-properties
    non-default-properties
```

Display

```
list quota-mgmt
list quota-mgmt [ [ [name] | [glob] | [regex] ] ... ]
show running-config quota-mgmt
show running-config quota-mgmt [ [ [name] | [glob] | [regex] ] ... ]
    all-properties
    non-default-properties
    one-line
    partition
```

Description

You can use the **quota-mgmt** component to configure global settings for quota management over Gy.

Examples

modify quota-mgmt default-rating-group rg_grp_1 service-context-id 32251@3gpp.org

Configures rg_grp_1 as default rating group and service-context-id as 32251@3gpp.org.
rg_grp_1 should be defined before.

list quota-mgmt

Displays the configuration for quota-mgmt.

Options

- **default-rating-group**
  Specifies the default rating group for quota management over Gy.
- **service-context-id**
  Specifies the service-context-id to be used for CCR message over Gy.

See Also

create, *delete*, *edit*, glob, *list*, *modify*, pem quota-mgmt rating-group, *listener*, *policy*, *diameter-endpoint*, *spm*, *format-script*, *service-chain-endpoint*, *subscriber*, *subscribers*, regex, *show*, *tmsh*

subscriber-activity-log

Configures the global settings that pertain to subscriber activity log messages for Policy Enforcement Manager (PEM).

Syntax

Modify the **subscriber-activity-log** component within the **pem global-settings** module using the syntax shown in the following sections.

Modify

```
modify subscriber-activity-log
    dynamic-subscriber-ids [add | delete | modify | replace-all-with] {
       [id_name ...]
    }
    dynamic-subscriber-ids [none]
    publisher [name]
    static-subscriber-ids [add | delete | replace-all-with] {
       [id_name ...]
    }
    static-subscriber-ids [default | none]
    subscriber-ip-addresses [add | delete | modify | replace-all-with] {
       [ip address/prefixlen ...]
    }
    subscriber-ip-addresses [none]
edit subscriber-activity-log [ [ [name] | [glob] | [regex] ] ... ]
    all-properties
    non-default-properties
reset-stats subscriber-activity-log
```

Display

```
list subscriber-activity-log
list subscriber-activity-log [ [ [name] | [glob] | [regex] ] ... ]
show running-config subscriber-activity-log
show running-config subscriber-activity-log [ [ [name] | [glob] | [regex] ] ... ]
    all-properties
    non-default-properties
    one-line
    partition
show subscriber-activity-log
    all-properties
    (default | exa | gig | kil | meg | peta | raw | tera | yotta | zetta)
    default
    field-fmt
```

Description

You can use the **subscriber-activity-log** component to monitor behavior of the subscribers in the troubleshooting mode by sending activity log messages to one or more destinations. You can add static and dynamic subscribers by IDs, or by subscriber IP addresses. The activity log messages contain the internal information exposing the subscribers behavior.

Examples

modify subscriber-activity-log publisher pub1 dynamic-subscriber-ids add { 4081112222 }

Adds dynamic subscriber 4081112222 to troubleshooting mode by sending activity log messages to all destinations defined in pub1.

list subscriber-activity-log

Displays the list of the subscribers in troubleshooting mode.

show subscriber-activity-log

Displays the logging statistics of the subscribers in troubleshooting mode.

reset-stats subscriber-activity-log

Resets the logging statistics of the subscribers in troubleshooting mode.

Options

- **dynamic-subscriber-ids**
  Specifies a list of dynamic subscriber IDs to be in troubleshooting mode.
- **publisher**
  Specifies the external logging publisher used to send activity log messages to one or more destinations.
- **static-subscriber-ids**
  Specifies a list of static subscriber IDs to be in troubleshooting mode.
- **subscriber-ip-addresses**
  Specifies a list of subscriber IP addresses to be in troubleshooting mode.

See Also

create, *delete*, *edit*, glob, *list*, *modify*, *forwarding-endpoint*, *interception-endpoint*, *listener*, *policy*, *diameter-endpoint*, *spm*, *format-script*, *service-chain-endpoint*, *subscriber*, *subscribers*, regex, *show*, *tmsh*

77

pem profile

- Introducing the PEM profile module
- Alphabetical list of components

Introducing the PEM profile module

You can use the tmsh components that reside within the Policy Enforcement Manager profile (pem profile) module to configure policy enforcement for the BIG-IP® system. For more information about the tmsh hierarchical structure, see Chapter 2, *Understanding and Using the Traffic Management Shell*.

Alphabetical list of components

The remainder of this chapter lists the tmsh components that are available in the pem profile module.

diameter-endpoint

Configures a diameter endpoint profile.

Syntax

Configures the **diameter-endpoint** profile within the **pem profile** module using the syntax shown in the following sections.

Modify

```
modify diameter-endpoint
    gx-endpoint {
        defaults-from [ [name] | none]
        destination-host [string]
        destination-realm [string]
        fatal-grace-time {
enabled [yes | no]
time [integer]
}
        msg-max-retransmits [integer]
        msg-retransmit-delay [integer]
        origin-host [string]
        origin-realm [string]
        product-name [string]
        supported-apps [Gx]
    }
}
edit diameter-endpoint [ [ [name] | [glob] | [regex] ] ... ]
    all-properties
    non-default-properties
reset-stats diameter-endpoint
reset-stats diameter-endpoint [ [ [name] | [glob] | [regex] ] ... ]
```

Display

```
list diameter-endpoint
list diameter-endpoint [ [ [name] | [glob] | [regex] ] ... ]
show running-config diameter-endpoint
show running-config diameter-endpoint [ [ [name] | [glob] | [regex] ] ... ]
    all-properties
    non-default-properties
    one-line
    partition
show diameter-endpoint
show diameter-endpoint [ [ [name] | [glob] | [regex] ] ... ]
     (default | exa | gig | kil | meg | peta | raw | tera | yotta | zetta)
     field-fmt
     global
```

Description

You can use the **diameter-endpoint** component to modify or display a diameter-endpoint profile.

Examples

modify gx-endpoint origin-host example-host.example-realm.org origin-realm example-realm destination-host example-peer.peer-realm.org destination-realm peer-realm.org

Sets the origin and destination of this diameter endpoint.

modify gx-endpoint msg-max-retransmits 8 msg-retransmit-delay 10000

Changes the maximum times a message will be retransmitted to 8 and changes the retransmission delay to 10 seconds.

Options

- **defaults-from**
  Specifies the name of the object to inherit the settings from.
- **destination-host**
  Specifies the destination host for diameter messages. This should be a FQDN.
- **destination-realm**
  Specifies the destination realm for diameter messages. This should be a FQDN.
- **fatal-grace-time**
  You can configure following options for fatal-grace-time. It defines the period that a diameter connection can be down before all sessions associated with that diameter endpoint are terminated. If the connection is re-established before **fatal-grace-time** seconds then the sessions will not be terminated automatically.
  - **enabled**
    Specifies whether fatal-grace-time option is enabled or no.
  - **time**

Specifies the fatal-grace-time period in seconds.

- **msg-max-retransmits**
  Specifies the number of times an outgoing request message will be retransmitted before being dropped.
- **msg-retransmit-delay**
  Specifies the delay in milliseconds after which an unanswered request will be retransmitted.
- **origin-host**
  Specifies the origin host for diameter messages. This should be a FQDN.

- **origin-realm**
  Specifies the origin realm for diameter messages. This should be a FQDN.
- **product-name**
  Specifies the string used in the product-name AVP in the capabilities exchange messages.
- **supported-apps**
  Adds, deletes, or replaces a set of the supported applications.

See Also

edit, glob, *list*, *virtual*, *modify*, *forwarding-endpoint*, *interception-endpoint*, *listener*, *policy*, *spm*, *format-script*, *service-chain-endpoint*, *subscriber*, *subscribers*, regex, *reset-stats*, *show*, *tmsh*

radius-aaa

Configures a PEM radius AAA profile.

Syntax

Configures the **radius-aaa** profile within the **pem profile** module using the syntax shown in the following sections.

Create/Modify

```
create radius-aaa [name]
modify radius-aaa [name]
    app-service [[string] | none]
    defaults-from [[name] | none]
    description [string]
    retransmission-timeout [integer]
    shared-secret [string]
    password [string]
    transaction-timeout [integer]
edit radius-aaa [ [ [name] | [glob] | [regex] ] ... ]
    all-properties
    non-default-properties
```

Display

```
list radius-aaa
list radius-aaa [ [ [name] | [glob] | [regex] ] ... ]
show running-config radius-aaa
show running-config radius-aaa [ [ [name] | [glob] | [regex] ] ... ]
    all-properties
    non-default-properties
    one-line
    partition
show radius-aaa
show radius-aaa [ [ [name] | [glob] | [regex] ] ... ]
     (default | exa | gig | kil | meg | peta | raw | tera | yotta | zetta)
     field-fmt
     global
```

Delete

```
delete radius-aaa [name]
```

Description

You can use the **radius-aaa** component to create, modify, display, or delete a radius-aaa profile.

Examples

create radius-aaa my_radius_aaa_profile

Creates a custom radius-aaa profile named **my_radius_aaa_profile**.

list radius-aaa my_radius_aaa_profile

Displays the properties of the radius-aaa profile named **my_radius_aaa_profile**.

Options

- **all**
  Specifies that you want to modify all of the existing components of the specified type.
- **defaults-from**
  Specifies the profile that you want to use as the parent profile. Your new profile inherits all settings and values from the parent profile. The default value is **radiusaaa**.
- **description**
  User defined description.
- **retransmission-timeout**
  Specifies the retransmission timeout value of the Radius-AAA profile in seconds.
- **shared-secret**
  Specifies the shared secret of the Radius-AAA profile when connecting to the RADIUS server.
- **password**
  Specifies the password of the Radius-AAA profile for authenticating to the RADIUS server.
- **transaction-timeout**
  Specifies the transaction timeout value of the Radius-AAA profile in seconds.
- **partition**
  Specifies the administrative partition within which the profile resides.

See Also

create, *delete*, *edit*, glob, *list*, *virtual*, *modify*, regex, *reset-stats*, *show*, *tmsh*

spm

Configures a Subscriber Policy Manager profile.

Syntax

Configures the **spm** profile within the **pem profile** module using the syntax shown in the following sections.

Create/Modify

```
create spm [name]
modify spm [name]
    app-service [[string] | none]
    defaults-from [[name] | none]
    description [string]
    global-policies-high-precedence [add | delete | replace-all-with] {
       [policy_name ...]
    }
    global-policies-high-precedence [ default | none ]
    global-policies-low-precedence [add | delete | replace-all-with] {
       [policy_name ...]
    }
    global-policies-low-precedence [ default | none ]
    unknown-subscriber-policies [add | delete | replace-all-with] {
       [policy_name ...]
    }
    unknown-subscriber-policies [ default | none ]
    fast-pem [enable | disable]
edit spm [ [ [name] | [glob] | [regex] ] ... ]
    all-properties
    non-default-properties
reset-stats spm
reset-stats spm [ [ [name] | [glob] | [regex] ] ... ]
```

Display

```
list spm
list spm [ [ [name] | [glob] | [regex] ] ... ]
show running-config spm
show running-config spm [ [ [name] | [glob] | [regex] ] ... ]
    all-properties
    non-default-properties
    one-line
    partition
show spm
show spm [ [ [name] | [glob] | [regex] ] ... ]
     (default | exa | gig | kil | meg | peta | raw | tera | yotta | zetta)
     field-fmt
     global
```

Delete

```
delete spm [name]
```

Description

You can use the **spm** component to create, modify, display, or delete a spm profile.

Examples

create spm my_spm_profile

Creates a custom spm profile named **my_spm_profile**.

list spm my_spm_profile

Displays the properties of the spm profile named **my_spm_profile**.

Options

- **all**
  Specifies that you want to modify all of the existing components of the specified type.
- **defaults-from**
  Specifies the profile that you want to use as the parent profile. Your new profile inherits all settings and values from the parent profile. The default value is **spm**.
- **description**
  User defined description.
- **global-policies-high-precedence**
  Adds, deletes, or replaces a set of the policies.
- **global-policies-low-precedence**
  Adds, deletes, or replaces a set of the policies.
- **unknown-subscriber-policies**
  Adds, deletes, or replaces a set of the policies.
- **fast-pem**
  Specifies whether fast PEM optimization is enabled or not. The default is **enabled**.
- **partition**
  Specifies the administrative partition within which the profile resides.

See Also

edit, glob, *list*, *virtual*, *modify*, *forwarding-endpoint*, *interception-endpoint*, *listener*, *policy*, *diameter-endpoint*, *format-script*, *service-chain-endpoint*, *subscriber*, regex, *reset-stats*, *show*, *tmsh*

78

pem quota management

- Introducing the PEM quota management module
- Alphabetical list of components

Introducing the PEM quota management module

You can use the tmsh components that reside within the Policy Enforcement Manager (PEM) quota management module to configure quota management for the PEM. For more information about the tmsh hierarchical structure, see Chapter 2, *Understanding and Using the Traffic Management Shell*.

Alphabetical list of components

The remainder of this chapter lists the tmsh components that are available in the pem quota management module.

rating-group

Configures a rating-group for quota management in Policy Enforcement Manager (PEM).

Syntax

Modify the **rating-group** component within the **pem quota-mgmt** module using the syntax shown in the following sections.

Create/Modify

```
create rating-group [name]
modify rating-group [name]
    app-service [[string] | none]
    rating-group-id [integer]
    definition [string]
    description [string]
    request-on-install [yes | no]
    default-threshold [integer]
    default-validity-time [integer]
    default-quota-holding-time [integer]
    initial-quota-request {
 interval [integer]
 volume {
            input-octets
     output-octets
     total-octets
}
    default-quota {
 interval [integer]
 volume {
            input-octets
     output-octets
     total-octets
}
       time {
    usage-time
           consumption-time
       }
    default-breach-action [terminate | allow | redirect]
    default-forwarding-endpoint [name]
edit rating-group [ [ [name] | [glob] | [regex] ] ... ]
    all-properties
    non-default-properties
```

Display

```
list rating-group
list rating-group [ [ [name] | [glob] | [regex] ] ... ]
show running-config rating-group
show running-config rating-group [ [ [name] | [glob] | [regex] ] ... ]
    all-properties
    non-default-properties
    one-line
    partition
```

Delete

```
delete rating-group [name]
```

Note

You must remove all references to a rating-group object before you can delete it.

Examples

```
create rating-group rg1 {
   rating-group-id 1
   initial-quota-request {
      volume {
          input-octets 1000
    output-octets 1000
    total-octets 2000
      }
   }
   default-quota {
      volume {
         input-octets 1000
   output-octets 1000
   total-octets 2000
      }
   }
   request-on-install yes
}
```

Creates a PEM rating-group named **rg1**.

delete rating-group rg1

Deletes the rating-group named **rg1**.

list rating-group rg1

Displays the properties of the rating-group named **rg1**.

Options

- **app-service**
  Specifies the name of the application service to which the object belongs. The default value is **none**. **Note:** If the **strict-updates** option is **enabled** on the application service that owns the object, you cannot modify or delete the object. Only the application service can modify or delete the object.
- **rating-group-id**
  Specifies the rating-group-id that will be used by quota managing endpoint. For instance, this could be the rating group in case of Gy endpoint.

- **request-on-install**
  Specifies whether quota has to be requested from the quota mangaing endpoint (Eg : Gy) when policy refererring this rating-group is installed for a subscriber or later when flow is initiated.
- **default-threshold**
  Specifies the default threshold if the quota managing endpoint does not specify threshold.
- **default-validity-time**
  Specifies the default validity time for the quota in seconds if OCS did not specify it.
- **default-quota-holding-time**
  Specifies the default quota holding time in seconds for which quota is valid without any usage if not specified by OCS.
- **initial-quota-request**
  Specifies the initial quota, that will be requested from the quota managing endpoint. Could be either time or volume.
  - **time**
    Specifies the time in seconds.
  - **volume**
    You can configure the following options for volume initial quota.
    - **output-octets**
      Specifies the initial quota for downlink traffic.
    - **total-octets**
      Specifies the initial quota for total uplink and downlink traffic.
    - **input-octets**
      Specifies the initial quota for uplink traffic.
- **default-quota**
  Specifies the default quota, that will be used if quota managing endpoint does not respond. Could be either time or volume.
  - **time**
    Specifies the quota in time.
    - **usage-time**
      Specifies the usage time in seconds.
    - **consumption-time**
      Specifies the quota consumption time in seconds.
  - **volume**
    You can configure the following options for volume default quota.
    - **output-octets**
      Specifies the default quota for downlink traffic.
    - **total-octets**
      Specifies the default quota for total uplink and downlink traffic.
    - **input-octets**
      Specifies the default quota for uplink traffic.

See Also

create, *delete*, *edit*, glob, *list*, *modify*, *policy*, *show*, *tmsh*

79

pem reporting

- Introducing the PEM Reporting module
- Alphabetical list of components

Introducing the PEM Reporting module

You can use the tmsh components that reside within the Policy Enforcement Manager (pem) reporting module to configure policy enforcement for the BIG-IP® system. For more information about the tmsh hierarchical structure, see Chapter 2, *Understanding and Using the Traffic Management Shell*.

Alphabetical list of components

The remainder of this chapter lists the tmsh components that are available in the pem reporting module.

format-script

Configures format scripts for the Policy Enforcement Manager (PEM).

Syntax

Modify the **format-script** component within the **pem reporting** module using the syntax shown in the following sections.

Create/Modify

```
create format-script [name]
modify format-script [name]
    app-service [[string] | none]
    definition [string]
    description [string]
edit format-script [ [ [name] | [glob] | [regex] ] ... ]
    all-properties
    non-default-properties
```

Display

```
list format-script
list format-script [ [ [name] | [glob] | [regex] ] ... ]
show running-config format-script
show running-config format-script [ [ [name] | [glob] | [regex] ] ... ]
    all-properties
    non-default-properties
    one-line
    partition
```

Delete

```
delete format-script [name]
```

◆ Note

You must remove all references to a format script object before you can delete it.

Description

You can use the **format-script** component to create scripts for HSL reporting. The scripts use TCL syntax and define a custom format that is applied in an enforcement policy rule. The format and fields available differ depending on whether the rule specifies session-based or flow-based reporting.

Examples

create format-script fm1 { definition { return "(flow app_id[PEM::flow stats reported app-id], bytes-in:[PEM::flow stats reported bytes-in])" } }

Creates a PEM reporting format script named **fm1**.

delete format-script fm1

Deletes the format script named **fm1**.

list format-script fm1

Displays the properties of the format script named **fm1**.

Options

- **app-service**
  Specifies the name of the application service to which the object belongs. The default value is **none**. **Note:** If the **strict-updates** option is **enabled** on the application service that owns the object, you cannot modify or delete the object. Only the application service can modify or delete the object.
- **definition**
  Specifies a script using TCL syntax that defines a custom format for HSL reporting applied in an enforcement policy rule. The format and fields available differ depending on whether you are using session-based or flow-based reporting in the rule.
  - **Session-based formats:**
    The options are:
    - **app-id**
      Specifies the application id of the session record.
    - **bytes-in**
      Specifies the aggregate incoming bytes of the session.
    - **bytes-out**
      Specifies the aggregate outgoing bytes of the session.
    - **last-send-sec**
      Specifies the value of seconds of the timestamp since the previous record was sent.
    - **last-send-usec**
      Specifies the value of microseconds of the timestamp since the previous record was sent.
    - **param-3gpp**
      Specifies the comma-separated string of the value of imsi, imeisv, tower-id, and user-name.
    - **rec-reason**
      Specifies the reason for sending report. The values are **1**: period time, **2**: volume threshold, **3**: subscriber logout, **4**: inactivity.

- **rec-type**
  Specifies the type of the session-based record (always **3**).
- **subs-id**
  Specifies the subscriber id.
- **subs-id-type**
  Specifies the subscriber id type (e164, imsi, nai, or private).
- **timestamp-sec**
  Specifies the seconds value of the timestamp when the record was generated. The Unix epoch is 1970-01-01T00:00:00Z.
- **timestamp-usec**
  Specifies the microseconds value of the timestamp when the record was generated.

- **Flow-based formats:**
  The options are:
  - **app-id**
    Specifies the application id of the flow record.
  - **bytes-in**
    Specifies the aggregate incoming bytes of the flow.
  - **bytes-out**
    Specifies the aggregate outgoing bytes of the flow.
  - **dst-ip**
    Specifies the destination ip address of the flow.
  - **dst-port**
    Specifies the destination port of the flow.
  - **proto**
    Specifies the protocol of the flow.
  - **rec-type**
    Specifies the type of the flow-based record. The value is **0**: flow init, **1**: flow interim, and **2**: flow end.
  - **src-ip**
    Specifies the source ip address of the flow.
  - **src-port**
    Specifies the destination port of the flow.
  - **subs-id**
    Specifies the subscriber id.
  - **subs-id-type**
    Specifies the subscriber id type (e164, imsi, nai, or private).
  - **flow-start-time-sec**
    Specifies the seconds value of the timestamp when the flow starts. The Unix epoch is 1970-01-01T00:00:00Z.
  - **flow-start-time-usec**
    Specifies microseconds value of the timestamp when the flow starts.

- **flow-end-time-sec**
  Specifies the seconds value of the timestamp when the flow ends. The Unix epoch is 1970-01-01T00:00:00Z.
- **flow-end-time-usec**
  Specifies microseconds value of the timestamp when the flow ends.
- **timestamp-sec**
  Specifies the of seconds value of the timestamp when the record was generated. The Unix epoch is 1970-01-01T00:00:00Z.
- **timestamp-usec**
  Specifies the microseconds value of the timestamp when the record was generated.

◆ **description**
Specifies a user-defined description.

See Also

create, *delete*, *edit*, glob, *list*, *modify*, *forwarding-endpoint*, *interception-endpoint*, *listener*, *policy*, *diameter-endpoint*, *spm*, *service-chain-endpoint*, *subscriber*, *subscribers*, regex, *show*, *tmsh*

80

pem stats

- Introducing the PEM stats module
- Alphabetical list of components

Introducing the PEM stats module

You can use the tmsh components that reside within the Policy Enforcement Manager (PEM) stats module to view policy enforcement statistics for the BIG-IP® system. For more information about the tmsh hierarchical structure, see Chapter 2, *Understanding and Using the Traffic Management Shell*.

Alphabetical list of components

The remainder of this chapter lists the tmsh components that are available in the pem stats module.

action

Displays and resets PEM policy action statistics.

Syntax

Display statistics for the **action** component within the **pem stats** module using the syntax in the following section.

Display

```
show action
  option:
    (default | exa | gig | kil | meg | peta | raw | tera | yotta | zetta)
```

Description

You can use the **action** component to display PEM policy action statistics. The statistics details are described below:

- **Pass**
  Specifies the number of flows that are passed (gate enabled).
- **Drop**
  Specifies the number of flows that are dropped (gate disabled).
- **Clone**
  Specifies the number of flows to which clone actions apply.
- **HTTP Redirect**
  Specifies the number of flows to which redirection actions apply.
- **ICAP Request**
  Specifies the number of flows to which ICAP actions apply on the request direction.
- **ICAP Response**
  Specifies the number of flows to which ICAP actions apply on the response direction.
- **Steering**
  Specifies the number of flows to which steering actions apply.
- **Service Chain**
  Specifies the number of flows to which steering endpoint actions apply.
- **Steering on Response**
  Specifies the number of flows to which steering actions apply on the response direction.
- **QoS Uplink**
  Specifies the number of uplink flows to which QoS actions apply. Uplink means to network.

- **QoS Downlink**
  Specifies the number of downlink flows to which QoS actions apply. Downlink means to subscriber.
- **DSCP Marking Uplink**
  Specifies the number of uplink flows with DSCP action applies.
- **DSCP Marking Downlink**
  Specifies the number of downlink flows with DSCP action applies.
- **HTTP Headers Modify**
  Specifies the number of HTTP Headers Modify actions.
- **iRule**
  Specifies the number of iRule actions.
- **L2 Marking Uplink**
  Specifies the number of uplink flows to which L2 Marking actions apply.
- **L2 Marking Downlink**
  Specifies the number of downlink flows to which L2 Marking actions apply.
- **Flow Reporting**
  Specifies the number of actions of flow reporting record generation applied.
- **Session Reporting**
  Specifies the number of actions of session record generation applied.
- **Transaction Reporting**
  Specifies the number of actions of transaction record generation applied.
- **Policy Re-evaluation Rate (count/min)**
  Specifies the number of successful policy reevaluations per minute.
- **Policy Re-evaluation Rate Maximum**
  Specifies the maximum number of policy reevaluations overall for all subscribers and flows.

You can reset the PEM policy action statistics using **reset-stats** command.

Examples

show action

Displays the PEM policy action statistics.

reset-stats action

Resets the PEM policy action statistics.

Options

For information about the options that you can use with the command **show**, see **help show**.

See Also

show, *gx*, *gy*, *hsl*, *radius*, *subscriber*, *tmsh*

gx

Displays and resets PEM gx statistics.

Syntax

Display statistics for the **gx** component within the **pem stats** module using the syntax in the following section.

Display

```
show gx
  option:
    (default | exa | gig | kil | meg | peta | raw | tera | yotta | zetta)
```

Description

You can use the **gx** component to display PEM gx statistics. The statistics details are described below:

- **Concurrent Sessions**
  Specifies the number of active Gx sessions established.
- **Concurrent Sessions Maximum**
  Specifies the maximum number of active Gx sessions observed since the last reset of the counter.
- **Sessions Created**
  Specifies the total number of Gx sessions observed since the last reset of the counter.
- **Non Provisioned Sessions**
  Specifies the current number of inactive Gx sessions for which provisioning or creation error happened.
- **Non Provisioned Sessions Maximum**
  Specifies the maximum number of inactive Gx sessions for which provisioning or creation error happened.
- **Provisioning Initiated**
  Specifies the current number sessions for which provisioning or creation over Gx has been initiated.
- **Provisioning Initiated Maximum**
  Specifies the maximum number sessions for which provisioning or creation over Gx has been initiated.
- **Error Messages Received**
  Specifies the number of erroneous messages or response with error code received (may be separated to two counters).
- **Termination Initiated**
  Specifies the current number of Gx sessions for which close is initiated.

- **Termination Initiated Maximum**
  Specifies the maximum number of Gx sessions for which close is initiated.
- **Sessions Terminated**
  Specifies the total number of Gx sessions terminated since the last reset of the counter.
- **CCR Sent**
  Specifies the number of CCR requests of all types sent.
- **CCA Received**
  Specifies the number of CCA responses of all types received.
- **CCR Initial Sent**
  Specifies the number of CCR Initial requests sent since the last reset of the counter.
- **CCA Initial Received**
  Specifies the number of CCA Initial responses received since the last reset of the counter.
- **CCR Update Sent**
  Specifies the number of CCR Update requests sent since the last reset of the counter.
- **CCA Update Received**
  Specifies the number of CCA Update responses received since the last reset of the counter.
- **RAR Received**
  Specifies the number of RAR received.
- **RAA Sent**
  Specifies the number of RAA sent.
- **CCR Usage Monitoring Sent**
  Specifies the number of CCR with usage monitoring report sent.
- **CCA Usage Monitoring Received**
  Specifies the number of CCA with usage monitoring report ack received.
- **CCR Termination Sent**
  Specifies the number of CCR Termination requests sent since the last reset of the counter.
- **CCA Termination Received**
  Specifies the number of CCA Termination responses received since the last reset of the counter.

You can reset the PEM gx statistics using **reset-stats** command.

Examples

show gx

Displays the PEM gx statistics.

reset-stats gx

Resets the PEM gx statistics.

Options

For information about the options that you can use with the command **show**, see **help show**.

See Also

show, *action*, *gy*, *hsl*, *radius*, *subscriber*, *tmsh*

gy

Displays and resets PEM gy statistics.

Syntax

Display statistics for the **gy** component within the **pem stats** module using the syntax in the following section.

Display

```
show gy
  option:
    (default | exa | gig | kil | meg | peta | raw | tera | yotta | zetta)
```

Description

You can use the **gy** component to display PEM gy statistics. The statistics details are described below:

- **Concurrent Sessions**
  Specifies the number of active Gy sessions established.
- **Concurrent Sessions Maximum**
  Specifies the maximum number of active Gy sessions observed since the last reset of the counter.
- **Sessions Created**
  Specifies the total number of Gy sessions observed since the last reset of the counter.
- **Non Provisioned Sessions**
  Specifies the current number of inactive Gy sessions for which provisioning or creation errors happen.
- **Non Provisioned Sessions Maximum**
  Specifies the maximum number of inactive Gy sessions for which provisioning or creation errors happen.
- **Provisioning Initiated**
  Specifies the current number of sessions for which provisioning or creation over Gy has been initiated.
- **Provisioning Initiated Maximum**
  Specifies the maximum number of sessions for which provisioning or creation over Gy has been initiated.
- **Error Messages Received**
  Specifies the number of erroneous messages or response with error code received (may be separated to two counters).
- **Termination Initiated**
  Specifies the current number of Gy sessions for which close is initiated.

- **Termination Initiated Maximum**
  Specifies the maximum number of Gy sessions for which close is initiated.
- **Sessions Terminated**
  Specifies the total number of Gy sessions terminated since the last reset of the counter.
- **CCR Sent**
  Specifies the number of CCR requests of all types sent.
- **CCA Received**
  Specifies the number of CCA responses of all types received.
- **CCR Initial Sent**
  Specifies the number of CCR Initial requests sent since the last reset of the counter.
- **CCA Initial Received**
  Specifies the number of CCA Initial responses received since the last reset of the counter.
- **CCR Update Sent**
  Specifies the number of CCR Update requests sent since the last reset of the counter.
- **CCA Update Received**
  Specifies the number of CCA Update responses received since the last reset of the counter.
- **RAR Received**
  Specifies the number of RAR received.
- **RAA Sent**
  Specifies the number of RAA sent.
- **CCR Termination Sent**
  Specifies the number of CCR Termination requests sent since the last reset of the counter.
- **CCA Termination Received**
  Specifies the number of CCA Termination responses received since the last reset of the counter.

You can reset the PEM gy statistics using **reset-stats** command.

Examples

show gy

Displays the PEM gy statistics.

reset-stats gy

Resets the PEM gy statistics.

Options

For information about the options that you can use with the command **show**, see **help show**.

See Also

show, *action*, *gx*, *hsl*, *radius*, *subscriber*, *tmsh*

hsl

Displays and resets PEM hsl statistics.

Syntax

Display statistics for the **hsl** component within the **pem stats** module using the syntax in the following section.

Display

```
show hsl
  option:
    (default | exa | gig | kil | meg | peta | raw | tera | yotta | zetta)
```

Description

You can use the **hsl** component to display PEM hsl statistics. The statistics details are described below:

- **Session Records**
  Specifies the number of Session-based records sent to each HSL endpoint since the last reset of the counter.
- **Flow Start Records**
  Specifies the number of Flow Start records sent to each HSL endpoint since the last reset of the counter.
- **Flow Interim Records**
  Specifies the number of Flow Interim records sent to each HSL endpoint since the last reset of the counter.
- **Flow Stop Records**
  Specifies the number of Flow Stop records sent to each HSL endpoint since the last reset of the counter.
- **Transaction Records**
  Specifies the number of HTTP Transaction records sent to each HSL endpoint since the last reset of the counter.
- **Records Skipped**
  Specifies the number of reporting records skipped from being sent the HSL endpoint since the last reset of the counter.

You can reset the PEM hsl statistics using **reset-stats** command.

Examples

show hsl

Displays the PEM hsl statistics.

reset-stats hsl

Resets the PEM hsl statistics.

Options

For information about the options that you can use with the command **show**, see **help show**.

See Also

show, *action*, *gx*, *gy*, *radius*, *subscriber*, *tmsh*

radius

Displays and resets PEM radius statistics.

Syntax

Display statistics for the **radius** component within the **pem stats** module using the syntax in the following section.

Display

```
show radius
  option:
    (default | exa | gig | kil | meg | peta | raw | tera | yotta | zetta)
```

Description

You can use the **radius** component to display PEM radius statistics. The statistics details are described below:

- **Accounting-Start**
  Specifies the number of Accounting-Start packets received.
- **Accounting-Stop**
  Specifies the number of Accounting-Stop packets received.
- **Accounting-Interim**
  Specifies the number of Accounting-Interim packets received.
- **Accounting-Retransmission**
  Specifies the number of Accounting-Retransmission packets received.

You can reset the PEM radius statistics using **reset-stats** command.

Examples

show radius

Displays the PEM radius statistics.

reset-stats radius

Resets the PEM radius statistics.

Options

For information about the options that you can use with the command **show**, see **help show**.

See Also

show, *action*, *gx*, *gy*, *hsl*, *subscriber*, *tmsh*

subscriber

Displays and resets PEM subscriber statistics.

Syntax

Display statistics for the **subscriber** component within the **pem stats** module using the syntax in the following section.

Display

```
show subscriber
  option:
    (default | exa | gig | kil | meg | peta | raw | tera | yotta | zetta)
```

Description

You can use the **subscriber** component to display PEM subscriber statistics. The statistics details are described below:

- **Concurrent Subscribers**
  Specifies the number of concurrent subscribers per device. Note that you can use the **db** component in the **sys** module to configure **tmm.pem.spm.maxsessionlimit** to set the number of subscribers supported per processing unit (TMM). Then, the max number of the subscribers per device is set accordingly.
- **Concurrent Subscribers Maximum**
  Specifies the max number of concurrent subscribers observed since the last reset of the counter.
- **Total Subscribers**
  Specifies the total number of established subscribers since the last reset of the counter.
- **Subscriber Limit Exceeded**
  Specifies the counter of the subscribers creation failures, which are caused by exceeding the max number of subscribers supported by one processing unit (TMM).
- **Failed Provisioning Attempts**
  Specifies the aggregated number of failed provisioning attempts for all subscribers in the system since the last reset of the counter. A provisioning attempt fails if a policy server (PCRF) returns an error, or does not respond for any reason.
- **No Radius info**
  Specifies the current number of dynamic subscribers triggered by the data traffic without receiving Radius accounting start.
- **No Radius Info Maximum**
  Specifies the max number of dynamic subscribers triggered by the data traffic without receiving Radius accounting start observed since the last reset of the counter.

- **Waiting For Provisioning**
  Specifies the number of current subscribers waiting for provisioning completed.
- **Waiting For Provisioning Maximum**
  Specifies the max number of subscribers waiting for provisioning completed observed since the last reset of the counter.
- **Not Provisioned**
  Specifies the number of current subscribers which are not provisioned.
- **Not Provisioned Maximum**
  Specifies the number of subscribers not provisioned since the last reset of the counter.
- **Unknown**
  Specifies the number of current subscribers with "Unknown Subscriber Policy" (non-provisioned from the PCRF). This counter aggregates the counters of subscribers in the state of "Waiting for Provisioning" and "Not Provisioned".
- **Unknown Maximum**
  Specifies the max number of subscribers with "Unknown Subscriber Policy" (non-provisioned from PCRF) since the last reset of the counter.
- **Provisioned**
  Specifies the number of currently provisioned subscribers.
- **Provisioned Maximum**
  Specifies the number of provisioned subscribers observed since the last reset of the counter.
- **Inactive Subscribers Removed**
  Specifies the number of subscribers removed due to inactivity timeout.
- **Marked For Deletion**
  Specifies the number of current subscribers marked for deletion for any reason.
- **Marked For Deletion Maximum**
  Specifies the max number of subscribers marked for deletion for any reason observed since the last reset of the counter.

You can reset the PEM subscriber statistics using **reset-stats** command.

Examples

show subscriber

Displays the PEM subscriber statistics.

reset-stats subscriber

Resets the PEM subscriber statistics.

Options

For information about the options that you can use with the command **show**, see **help show**.

See Also

show, *action*, *gx*, *gy*, *hsl*, *radius*, *tmsh*

81

security analytics

- Introducing the security analytics module
- Alphabetical list of components

Introducing the security analytics module

You can use the tmsh components that reside within the security analytics module to modify the analytics for the Advanced Firewall Module (AFM). For more information about the tmsh hierarchical structure, see Chapter 2, *Understanding and Using the Traffic Management Shell*.

Alphabetical list of components

The remainder of this chapter lists the tmsh components that are available in the security analytics module.

settings

Configure global settings for security (AFM) analytics.

Syntax

Configure the **settings** component within the **security analytics** module using the syntax shown in the following sections.

Modify

```
modify settings
    acl-rules {
      collect-client-ip [enabled | disabled]
      collect-client-port [enabled | disabled]
      collect-dest-ip [enabled | disabled]
      collect-dest-port [enabled | disabled]
      collect-server-side-stats [enabled | disabled]
    }
    collected-stats-internal-logging [enabled | disabled]
    collected-stats-external-logging [enabled | disabled]
    dns {
      collect-client-ip [enabled | disabled]
    }
    dos-l2-l4 {
      collect-client-ip [enabled | disabled]
    }
    l3-l4-errors {
      collect-client-ip [enabled | disabled]
      collect-dest-ip [enabled | disabled]
    }
    publisher [name]
    smtp-config [name]
    stale-rules {
      collect [enabled | disabled]
    }
```

Display

```
list settings
```

Description

Use the **settings** component to modify the settings for analytics entity collection for the AFM (advanced firewall) module.

Examples

modify settings acl-rules { collect-client-ip disabled }

Disables source/client IP analytics collection for ACL rules.

list settings

Displays analytics settings for AFM.

Options

- **acl-rules**
  Firewall (ACL) security statistics collection options.
  - **collect-client-ip**
    Specifies whether source/client IP address should be collected for ACL rule matching.
  - **collect-client-port**
    Specifies whether source/client port should be collected for ACL rule matching.
  - **collect-dest-ip**
    Specifies whether the destination IP address should be collected for ACL rule matching.
  - **collect-dest-port**
    Specifies whether the destination port should be collected for ACL rule matching.
  - **collect-server-side-stats**
    Specifies whether server side statistics (source address translation information, self IP address and pool member address) should be collected for ACL rule matching.
- **collected-stats-internal-logging**
  Enables or disables the internal logging of the collected statistics.
- **collected-stats-external-logging**
  Enables or disables the external logging of the collected statistics.
- **dns**
  DNS security statistics collection options.
  - **collect-client-ip**
    Specifies whether source/client IP address should be collected for DNS security.
- **dos-l2-l4**
  Network DoS security statistics collection options.
  - **collect-client-ip**
    Specifies whether source/client IP address should be collected for network layer's DoS security.
- **l3-l4-errors**
  Firewall errors statistics collection options.
  - **collect-client-ip**
    Specifies whether source/client IP address should be collected for firewall errors.
  - **collect-dest-ip**
    Specifies whether the destination IP address should be collected for firewall errors.

- **publisher**
  Specifies the external logging publisher used to send statistical data to one or more destinations.
- **smtp-config**
  Specifies the default SMTP configuration used for exporting CSV or PDF security analytics reports.
- **stale-rules**

  - **collect**
    Specifies whether statistics about all firewall rules should be collected in order to present information regarding rule staleness.

See Also

list, *modify*, *show*, *tmsh*, *analytics network*, *analytics dos-l3*, *analytics dns-dos*, *analytics dns-protocol*

82

security anti-fraud

- Introducing the security anti-fraud module
- Alphabetical list of components

Introducing the security anti-fraud module

You can use the tmsh components that reside within the security anti-fraud module to modify the anti-fraud profile for the Advanced Firewall Module (AFM). For more information about the tmsh hierarchical structure, see Chapter 2, *Understanding and Using the Traffic Management Shell*.

Alphabetical list of components

The remainder of this chapter lists the tmsh components that are available in the security anti-fraud module.

profile

Configures a Fraud Protection Service profile.

Syntax

Configure the **profile** component within the **security anti-fraud** module using the syntax shown in the following sections.

Create/Modify

```
create profile [name]
modify profile [name]
    app-service [[string] | none]
      name [string] {
           alert-identifier  [string]
           alert-path  [string]
           alert-pool  [string]
           alert-publisher  [string]
           app-service  [string]
           auto-transactions  [none | add | delete | modify | replace-all-with] {
               bot-score [integer]
               click-score [integer]
               integrity-fail-score [integer]
               min-mouse-move-count [integer]
               min-mouse-over-count [integer]
               min-report-score [integer]
               min-time-to-request [integer]
               not-human-score [integer]
               score-tampered-cookie [integer]
               time-fail-score [integer]
           }
   [case-sensitive | case-insensitive]
   check-path-info [enabled | disabled]
   cookies   [none | add | delete | modify | replace-all-with] {
       components-state [string]
       encryption-disabled [string]
       malware-cache [string]
       malware-counter [string]
       malware-guid [string]
       phishing-cache [string]
       secure-channel [string]
       transaction-data [string]
       user-inspection [string]
       user-name [string]
   }
   description [string]
   malware   [none | add | delete | modify | replace-all-with] {
       allowed-domains [string]
       bait-content [string]
       bait-location [string]
       blacklist-words  { [string] ... }
       flash-cookie-content [string]
       flash-cookie-location [string]
       flash-cookies [enabled | disabled]
       source-integrity-location [string]
   }
```

```
   phishing  [none | add | delete | modify | replace-all-with] {
       allowed-elements  [string]
       allowed-referrers  [string]
       css-attribute-name  [string]
       css-content  [string]
       css-location  [string]
       image-location  [string]
       protected-elements  [string]
       referrer-checks [enabled | disabled]
   }
   inspected-users [none | add | delete | modify | replace-all-with]  { [string] ... }
}
edit profile [ [ [name] | [glob] | [regex] ] ... ]
    all-properties
    non-default-properties
```

Display

```
list profile
list profile [ [ [name] | [glob] | [regex] ] ... ]
show anti-fraud profile
show anti-fraud profile [ [ [name] | [glob] | [regex] ] ... ]
    all
    auto-transactions
    cookies
    malware
    phishing
```

Delete

```
delete profile [name]
```

Description

You can use the **profile** component to create, modify, display, or delete a Anti-Fraud profile.

Examples

create profile my_dos_profile

Creates a custom Anti-Fraud profile named **myanti-fraud_profile** with default parameters.

list profile

Displays the properties of all Anti-Fraud profiles.

Options

- **alert-identifier**
  Specifies Unique account identifier.

- **alert-path**
  URL path that will receive alerts
- **alert-pool**
  Pool that will receive alerts
- **alert-publisher**
  Publisher that will receive alerts
- **auto-transactions**
  Bot detection.
  - **bot-score**
    Value added to risk score if bot detected
  - **click-score**
    Value added to risk score if too few clicks are detected
  - **integrity-fail-score**
    Value added to risk score if parameters are found to have been tampered with after submit
  - **min-mouse-move-count**
    Value added to risk score if too few mouse moves are detected
  - **min-mouse-over-count**
    Minimum mouse moves expected
  - **min-report-score**
    Report automatic transaction if this score is exceeded
  - **min-time-to-request**
    Minimum time expected for human to fill in and send form
  - **not-human-score**
    Value added to risk score if user is possibly not a human
  - **score-tampered-cookie**
    Value added to risk score if cookie is tampered with
  - **time-fail-score**

  - **cookies**
    Names of cookies
    - **components-state**
      Cookie that contains FPS health check information
    - **encryption-disabled**
      Cookie that signals that encryption is disabled
    - **malware-cache**
      Cookie that contains hashes of past malware alerts
    - **malware-counter**
      Cookie that records which generic malware has been targeted by the honeypot
    - **malware-guid**
      Cookie that contains random user ID
    - **phishing-cache**
      Cookie that contains hashes of past phishing alerts

- **secure-channel**
  Source Integrity confirmation data cookie
- **transaction-data**
  Cookie that contains transaction integrity data.
- **user-inspection**
  Cookie that signals that user is to be inspected.
- **user-name**

- **malware**
  Malware detection configurations
- **phishing**
  Phishing site detection configurations
- **url**
  Pages to protect

83

security datasync

- Introducing the security datasync module
- Alphabetical list of components

Introducing the security datasync module

You can use the tmsh components that reside within the security datasync module to set up your datasync framework. For more information about the tmsh hierarchical structure, see Chapter 2, *Understanding and Using the Traffic Management Shell*.

Alphabetical list of components

The remainder of this chapter lists the tmsh components that are available in the security datasync module.

device-stats

Display the Datasync Framework device stats.

Syntax

Display the **device-stats** component within the **security datasync** module using the syntax shown in the following sections.

Display

```
list device-stats
list device-stats [ [ [name] | [glob] | [regex] ] ... ]
show running-config device-stats
show running-config device-stats [ [ [name] | [glob] | [regex] ] ... ]
    all-properties
    non-default-properties
    one-line
    partition
    recursive
```

Description

You can use the **device-stats** component to display the datasync device-stats for that are updated by the Datasync Framework.

Options

- **device**
  Displays the device name reflected by the stats.
- **table**
  Displays the table type reflected by the stats.
- **profile-chksum**
  Displays the checksum of the current active profile.
- **activation-epoch**
  Displays the activation epoch of the current active generation.
- **rows-available**
  Displays the number of available rows in the current active buffer.
- **rows-in-use**
  Displays the number of rows that are in use in the current active buffer.

See Also

create, *delete*, *edit*, glob, *list*, *modify*, regex, *show*, *tmsh*, trust-domain

global-profile

Manage the Datasync Framework settings that are globally synced across devices.

Syntax

Manage the **global-profile** component within the **security datasync** module using the syntax shown in the following sections.

Create/Modify

```
create global-profile [name]
modify global-profile [name]
    table [name]
    activation-epoch [ auto | [integer] ]
    deactivation-epoch [ deactivated | always-active | [integer] ]
    min-rows [ default | [integer] ]
    max-rows [ default | [integer] ]
    regen-time-offset [ default | [integer] ]
    regen-interval [ default | none | [integer] ]
    grace-time [ default | [integer] ]
    master-key [string]
    scramble-alg [string]
    hash-alg [string]
    mac-alg [string]
    mode-of-op [string]
    rsa-exp [ none | rsa-3 | rsa-f4 | default ]
    rsa-bits [ default | none | [integer] ]
    params [string]
edit global-profile [ [ [name] | [glob] | [regex] ] ... ]
    all-properties
    non-default-properties
```

Display

```
list global-profile
list global-profile [ [ [name] | [glob] | [regex] ] ... ]
show running-config global-profile
show running-config global-profile [ [ [name] | [glob] | [regex] ] ... ]
    all-properties
    non-default-properties
    one-line
    partition
    recursive
```

Delete

```
delete global-profile [name]
```

Description

You can use the **global-profile** component to create, modify, display, or delete a datasync global-profile for use with the Datasync Framework. All global-profiles must reside in the automatically created /Common/datasync-global folder. These profiles are synced across all of the devices in the trust domain using the manually-synced device-group **datasync-global-dg**.

WARNING

Creating, modifying or deleting global-profiles may result in the system being offline, in the case of a bad configuration.

Examples

create global-profile /Common/datasync-global/my_global_profile table table_name

Creates a custom datasync global-profile named **my_global_profile** for table **table_name** with initial settings, a random master-key, and an activation-epoch 30 minutes in the future.

list global-profile /Common/datasync-global/*

Displays the properties of all datasync global-profiles.

Options

- **table**
  Specifies the table to which the profile belongs.
- **activation-epoch**
  Specifies the epoch at which the profile becomes active, in UNIX-time.
- **deactivation-epoch**
  Specifies the epoch at which the profile becomes inactive, in UNIX-time.
- **create-timestamp**
  Displays the timestamp at which the profile was created, in UNIX-time.
- **min-rows**
  Specifies the minimum number of rows to generate before going online.
- **max-rows**
  Specifies the maximum number of rows to generate.
- **regen-time-offset**
  Specifies the time offset at which regeneration will be done, in seconds.
- **regen-interval**
  Specifies the time interval at which regeneration will be done, in seconds.
- **grace-time**
  Specifies the grace time during which new buffers are supported, but not yet activated, in seconds.

- **master-key**
  Specifies the secured master key upon which all cryptography is based. Use "auto" to generate a random key.
- **scramble-alg**
  Specifies the scrambling algorithm to use.
- **hash-alg**
  Specifies the hashing algorithm to use.
- **mac-alg**
  Specifies the MAC algorithm to use.
- **mode-of-op**
  Specifies the scrambling mode-of-operation to use.
- **rsa-exp**
  Specifies the RSA exponent.
- **rsa-bits**
  Specifies the number of bits to use for RSA keys.
- **params**
  Specifies additional internal parameters.

See Also

create, *delete*, *edit*, glob, *list*, *modify*, regex, *show*, *tmsh*, trust-domain

local-profile

Manage the Datasync Framework settings that are local, and not synced across devices.

Syntax

Manage the **local-profile** component within the **security datasync** module using the syntax shown in the following sections.

Modify

```
modify local-profile [table_name]
    buf-size [integer]
    ds-area [ none | asm | fps ]
    rows-bulk [integer]
    gen-timeout-sec [integer]
    min-mem-mb [integer]
    min-cpu-percent [integer]
    max-gen-rows [ infinite | [integer] ]
    keep-conf-files [integer]
    gen-pause-sec [integer]
    offline-until-gen [ enable | disable ]
edit local-profile [table_name]
    all-properties
    non-default-properties
```

Display

```
list local-profile
list local-profile [table_name]
show running-config local-profile
show running-config local-profile [ [ [name] | [glob] | [regex] ] ... ]
    all-properties
    non-default-properties
    one-line
    partition
    recursive
```

Description

You can use the **local-profile** component to modify or display a datasync local-profile for use with the Datasync Framework. Each profile is for a single table. The profiles cannot be created or deleted, only modified. These profiles are local; they are not synced across devices.

Options

- **buf-size**
  Specifies the size of each buffer in the table, in bytes.

- **ds-area**
  Specifies the memory area on which the table will be allocated.
- **rows-bulk**
  Specifies the number of rows to generate in each bulk.
- **gen-timeout-sec**
  Specifies the timeout of running the external generator per single bulk.
- **min-mem-mb**
  Specifies the minimum available memory in MB to start generator in non-urgent mode.
- **min-cpu-percent**
  Specifies the minimum available CPU percent to start generator in non-urgent mode.
- **max-gen-rows**
  Specifies the maximum rows to generate.
- **keep-conf-files**
  Specifies the number of configuration files to keep when rolling old ones.
- **gen-pause-sec**
  Specifies the time in seconds to pause between each bulk generation when in non-urgent mode.
- **offline-until-gen**
  Specifies if the system should be offline until the table is generated.

See Also

edit, *list*, *modify*, *show*, *tmsh*

84

security dos

- Introducing the security dos module
- Alphabetical list of components

Introducing the security dos module

You can use the tmsh components that reside within the security dos module to create a profile for defending against Denial-of-Service (DoS) attacks. For more information about the tmsh hierarchical structure, see Chapter 2, *Understanding and Using the Traffic Management Shell*.

Alphabetical list of components

The remainder of this chapter lists the tmsh components that are available in the security dos module.

device-config

Configures the global network DoS profile.

Syntax

Configure the global network DoS profile component within the **security dos** module using the syntax shown in the following sections.

Modify

```
modify device-config dos-device-config
    dos-device-vector {
      [vector type] {
        default-internal-rate-limit [integer | infinite]
        detection-threshold-percent [integer | infinite]
        detection-threshold-pps [integer | infinite]
      }
      ...
    }
    log-publisher [name]
reset-stats device-config
```

Display

```
list device-config
show running-config device-config
    all-properties
    dos-device-vector
    log-publisher
show device-config
```

Description

This component is used to modify or display the global device DoS profile and statistics for use with network DoS Protection functionality.

Examples

modify device-config ...

Modifies the global DoS profile settings.

list device-config

Displays all the properties of the device DoS profile.

Options

- **dos-device-vector**
  Configures attack detection thresholds and rate limit parameters for network DoS vectors.
- **log-publisher**
  Specifies the name of the log publisher which logs translation events. See **help sys log-config** for more details on the logging sub-system.

Vector Types

- **arp-flood**
  ARP Flood.
- **bad-ext-hdr-order**
  IPv6 extension headers in packet are out of order.
- **bad-icmp-chksum**
  Bad ICMP checksum.
- **bad-icmp-frame**
  Bad ICMP frames. To see the various reasons why ICMP frames are classified as bad, please refer to the written documentation.
- **bad-igmp-frame**
  Bad IGMP frames. To see the various reasons why IGMP frames are classified as bad, please refer to the written documentation.
- **bad-ip-opt**
  IPv4 option with illegal length.
- **bad-ipv6-hop-cnt**
  Bad IPv6 hop count. Terminated packet (cnt==0). Dropped when the rate hits rate limit.
- **bad-ipv6-ver**
  Bad IPv6 version. IP Version in the IPV6 packet is not 6.
- **bad-tcp-chksum**
  Bad TCP checksum.
- **bad-tcp-flags-all-clr**
  Bad TCP flags (all TCP header flags cleared).
- **bad-tcp-flags-all-set**
  Bad TCP flags (all flags set).
- **bad-ttl-val**
  Bad IP TTL value (TTL == 0 for IPv4).
- **bad-udp-chksum**
  Bad UDP checksum.
- **bad-udp-hdr**
  Bad UDP header. To see the various reasons why UDP headers are classified as bad, please refer to the written documentation.
- **bad-ver**
  Bad IP version 4. IPv4 version in IP header is not 4.

- **dns-any-query**
  DNS any query packet.
- **dns-a-query**
  DNS A query packet.
- **dns-ptr-query**
  DNS PTR query packet.
- **dns-ns-query**
  DNS NS query packet.
- **dns-soa-query**
  DNS SOA query packet.
- **dns-cname-query**
  DNS CNAME query packet.
- **dns-mx-query**
  DNS MX query packet.
- **dns-aaaa-query**
  DNS AAAA query packet.
- **dns-txt-query**
  DNS TXT query packet.
- **dns-srv-query**
  DNS SRV query packet.
- **dns-axfr-query**
  DNS AXFR query packet.
- **dns-ixfr-query**
  DNS IXFR query packet.
- **dns-malformed**
  DNS Malformed packet.
- **dns-other-query**
  DNS OTHER query packet.
- **dns-oversize**
  DNS packet with size > <tunable>. This sys db tunable is configurable with Dos.MaxDNSframeSize.
- **dup-ext-hdr**
  Duplicate IPv6 extension headers.
- **ether-brdcst-pkt**
  Ethernet broadcast packet.
- **ether-mac-sa-eq-da**
  Ethernet MAC SA == DA.
- **ether-multicast-pkt**
  Ethernet multicast packet.
- **ext-hdr-too-large**
  IPv6 extension header size too large. The max IPV6 extension header size is configurable via the sys db variable dos.maxipv6extsize.
- **fin-only-set**
  TCP header with only the FIN flag set.

- **flood**
  A Flood is an attack where multiple (typically many) endpoints initiate network traffic to a single subnet or recieving endpoint.
- **hdr-len-gt-l2-len**
  Header length > L2 length. No room in L2 packet for IPv4 header (including options).
- **hdr-len-too-short**
  Header length too short. IPv4 header length in IP header is less than 20 bytes.
- **hop-cnt-leq-one**
  IPv6 hop count <= <tunable> and the packet needs to be forwarded. This sys db tunable is configurable by the sys db variable tm.minipv6hopcnt.
- **host-unreachable**
  ICMP packets of type "Host Unreachable".
- **icmp-frag-flood**
  ICMP fragments flood.
- **icmp-frame-too-large**
  Packets larger than the maximum ICMP frame size. The max ICMP frame size is configurable via the sys db variable dos.maxicmpframesize.
- **icmpv4-flood**
  ICMPv4 Flood.
- **icmpv6-flood**
  ICMPv6 Flood.
- **igmp-flood**
  IGMP Flood.
- **igmp-frag-flood**
  IGMP Fragment Flood.
- **ip-bad-src**
  IP src addr is a broadcast or multicast address.
- **ip-err-chksum**
  IP error checksum. IPv4 header checksum error.
- **ip-frag-flood**
  IPv4 fragment flood.
- **ip-len-gt-l2-len**
  IP length > L2 length. Total length in IPv4 header is greater than the L3 part length in L2 packet.
- **ip-overlap-frag**
  IPv4 overlapping fragments.
- **ip-short-frag**
  IPv4 fragments whose payload size is less than the minimum IPv4 Fragment size. The minimum size is configurable via the db variable tm.minipfragsize.
- **ip-opt-frames**
  IP option frames. IPv4 packets with options. db variable tm.acceptipoptions must be enabled to receive IP options.

- **ip-other-frag**
  The total IPv4 fragments' size has exceeded the reassembly queue or the maximum IP packet size.
- **ipv6-atomic-frag**
  IPv6 frame with frag extension hdr, but the MF and offset fields are both 0.
- **ipv6-bad-src**
  IPv6 src addr is a multicast address.
- **ipv6-ext-hdr-frames**
  IPv6 extended header frames.
- **ipv6-frag-flood**
  IPv6 fragment flood.
- **ipv6-len-gt-l2-len**
  IPv6 length > L2 length.
- **ipv6-other-frag**
  The total IPv6 fragments' size has exceeded the reassembly queue or the maximum IP packet size.
- **ipv6-overlap-frag**
  IPv6 overlapping fragments.
- **ipv6-short-frag**
  IPv6 fragments whose payload size is less than the minimum IPv6 Fragment size. The minimum size is configurable via the db variable tm.minipv6fragsize.
- **land-attack**
  Land Attack. IP Src Address equals IP Dst Address. Both V4 and V6 are counted.
- **l2-len-ggt-ip-len**
  L2 length >> IP length. L2 packet length is much greater than payload length in IPv4 (L2 length > IP length and L2 length > minimum packet size).
- **l4-ext-hdrs-go-end**
  No L4 (extended headers go to or past the end of frame).
- **no-l4**
  No L4. No L4 payload for IPv4.
- **opt-present-with-illegal-len**
  TCP Option present with illegal length.
- **payload-len-ls-l2-len**
  Payload length < L2 length. Payload length in IPv6 header is less than L3 part length in L2 packet.
- **routing-header-type-0**
  Routing header type 0 present.
- **sip-malformed**
  SIP malformed packet
- **sip-invite-method**
  SIP INVITE method packet.

- **sip-ack-method**
  SIP ACK method packet.
- **sip-options-method**
  SIP OPTIONS method packet.
- **sip-bye-method**
  SIP BYE method packet.
- **sip-cancel-method**
  SIP CANCEL method packet.
- **sip-register-method**
  SIP REGISTER method packet.
- **sip-publish-method**
  SIP PUBLISH method packet.
- **sip-notify-method**
  SIP NOTIFY method packet.
- **sip-subscribe-method**
  SIP SUBSCRIBE method packet.
- **sip-message-method**
  SIP MESSAGE method packet.
- **sip-prack-method**
  SIP PRACK method packet.
- **sip-other-method**
  SIP OTHER method packet.
- **sweep**
  A Sweep is an attack where a single endpoint initiates network traffic to a large number of recieving endpoints or subnets.
- **syn-and-fin-set**
  SYN && FIN set.
- **tcp-ack-flood**
  TCP packets with the ACK flag set (for non-existing flows).
- **tcp-bad-urg**
  TCP packets with the URG flag set but URG pointer is 0.
- **tcp-hdr-len-gt-l2-len**
  TCP header length > L2 length. No room in packet for TCP header (including options).
- **tcp-hdr-len-too-short**
  TCP header length too short (length < 5). The offset field in TCP header is less than 20 bytes.
- **tcp-opt-overruns-tcp-hdr**
  TCP option overruns TCP header.
- **tcp-syn-flood**
  TCP header with only the SYN flag set.
- **tcp-synack-flood**
  TCP header with only the SYN and ACK flags set.
- **tcp-rst-flood**
  TCP header with only the RST flag set.

- **tcp-window-size**
  TCP non-RST pkt with window size < <tunable>. This sys db tunable is configurable with Dos.TcpLowWindowSize.
- **tidcmp**
  ICMP source quench packets.
- **too-many-ext-hdrs**
  Too many extended headers. The IPv6 extended headers are more than 4. This number can be set through db variable dos.maxipv6exthdrs.
- **ttl-leq-one**
  TTL <= <tunable>. For IPv4 forwarding. This sys db tunable is configurable by tm.minipttl.
- **unk-tcp-opt-type**
  Unknown TCP option type.
- **udp-flood**
  UDP Flood.UDP flood vector counts any UDP packets that either match the UDP Port InclusionList or donot match the UDP Port ExclusionList. "tmsh modify security dos udp-portlist" can be used to configure the udp port list.For more info about udp portlist and how to configure it use "help security dos udp-portlist"
- **unk-ipopt-type**
  Unknown IP option type.

Parameters

- **default-internal-rate-limit**
  This parameter is programmed in hardware to limit the traffic to BIG-IP software. If the hardware DoS support does not exist software uses **default-internal-rate-limit** to limit the good traffic (most of them are flood) to external servers. Bad packets are always dropped.
  If the rate limit value is infinite the rate limit is disabled.
- **detection-threshold-percent**
  This parameter specifies relative threshold that uses dynamically learned 1-hour average rate to detect attacks. If the current rate (1-minute average) increases the specified percent over the 1-hour average rate, attack is detected.
  If the threshold value is infinite the detection is disabled.
- **detection-threshold-pps**
  This parameter specifies absolute threshold value. If the current rate (1-minute average) is equal or above the threshold value, attack is detected.
  If the threshold value is infinite the detection is disabled.
- **packet-types**
  This parameter is used to specify type of packets that will be classified as Sweep/Flood attacks. There are various types of packet types that can be specified.

See Also

list, *modify*, security, *security dos*, *show*, *tmsh*

network-whitelist

Configures the DoS network whitelist component within the **security dos** module using the syntax shown in the following sections. These DoS network whitelist entries are applied to all packets except those going through the management interface.

Syntax

Modify

```
modify network-whitelist dos-network-whitelist
  description [string]
  entries [add | delete | modify | replace-all-with] {
     [ [name] ] {
        description [string]
        destination {
          address [ip_address/prefixlen]
          port [port]
        }
        ip-protocol [any | icmp | igmp | tcp | udp]
        source {
          address [ip_address/prefixlen] ]
          vlans [vlan name | vlanid/mask]
        }
     }
  }
```

Display

```
list network-whitelist
```

Description

You can use the **network-whitelist** component to configure a DoS network whitelist of upto eight entries for all traffic except the management interface. The HSB hardware compares all incoming traffic to the **network-whitelist** entries. If a match is found then it does not do DoS vector checks for those packets. If a match is not found then DoS vector checks are done on those packets. The network software does its regular DoS vector checks on the incoming packets as usual. If a DoS vector is hit then it compares that packet with the DoS **network-whitelist** entries. If the packet matches an entry, then the system does not increment the DoS vector that matched. If the packets does not match a DoS **network-whitelist** entry then the matched DoS vector is incremented and appropriate action is taken.

If an entry specifies more than one of the above items, a packet must pass *all* of the items to successfully match. For example, if an entry specifies a source subnet and a destination port, a packet must originate from the given subnet and must also have the specified destination port.

Either destination ip_address/prefixlen or source ip_address/prefixlen can be specified in a network-whitelist entry. An ip_address/prefixlen for both source and destination cannot be specified for an entry.

Examples

modify network-whitelist dos-network-whitelist description "bad interfaces" entries add { re_telnet { ip-protocol tcp destination { port telnet } } }

Creates a new entry called re_telnet. It matches any TCP packet whose destination port is telnet.

modify network-whitelist dos-network-whitelist entries add { internal-net { source { address 172.27.0.0/16 } } }

Creates an entry that matches traffic from the 172.27.0.0 network.

```
list network-whitelist
security dos network-whitelist dos-network-whitelist {
   entries {
       re_telnet {
           ip-protocol tcp
           destination {
               port telnet
           }
       }
       internal-net {
           source {
               address 172.27.0.0/16
           }
       }
   }
}
```

Displays the current list of DoS whitelist entries.

modify network-whitelist dos-network-whitelist entries delete { internal-net }

Removes the "internal-net" entry from the list of **network-whitelist** entries.

Options

- **description**
  Your description for the DoS **network-whitelist** entries.
- **entries**
  Adds, deletes, or replaces a **network-whitelist** entry.
  - **add**
    Creates a new entry, which you specify next with a unique string in curly braces ({}).
  - **delete**
    Deletes the entry that you specify next, in curly braces ({}). You can use **delete {all}** to empty the list of **network-whitelist** entries, which has the same effect as using **none** (see below).

- **modify**
  Modifies the existing entry that you specify next, in curly braces ({}). After the entry name, enter the new configuration settings for the entry inside a nested set of curly braces.
- **replace-all-with**
  Replaces the current set of **network-whitelist** entries with the entry(s) that you specify next, in curly braces ({}).
- **none**
  Empties the list of network-whitelist entries.

Enter the name of a entry to be added or modified, then enter an open curly brace ({), one or more of the following options, and a closed curly brace (}).

- **description**
  Your description for the current entry.
- **destination**
  Matches against each packet's destination IP and/or destination port.
  - **address**
    Specifies an IP address and network to compare against the packet's destination address.
    The format for an IPv4 address is *a*. *b*. *c*. *d* [/ *prefix*]. The general format for an IPv6 address is *a*: *b*: *c*: *d*: *e*: *f*: *g*: *h* [/ *prefix*]; you can shorten this by eliminating leading zeros from each field (for example, you can shorten "2001:0db7:3f4a:09dd:ca90:ff00:0042:8329" to "2001:db7:3f4a:9dd:ca90:ff00:42:8329"), and/or by removing the longest contiguous field of zeros (for example, you can shorten "2001:0:0:0:c34a:0:23ff:678" to "2001::c34a:0:23ff:678"). TMSH accepts any valid text representation of IPv6 addresses, as defined in RFC 2373 (see http://www.ietf.org/rfc/rfc2373.txt).
  - **port**
    Specifies a port to compare against the packet's destination port.
- **ip-protocol**
  Specifies the IP protocol to compare against the packet. This could be **any**, **icmp**, **igmp**, **tcp** or **udp**. If you specify this option, a packet only matches if it uses the chosen protocol.
- **source**
  Matches against each packet's source IP, and/or source VLANs.
  - **address**
    Specifies an IP address and network to compare against the packet's source address.
    The format for an IPv4 address is *a*. *b*. *c*. *d*. The general format for an IPv6 address is *a*: *b*: *c*: *d*: *e*: *f*: *g*: *h*.
  - **vlans**
    Specifies either a vlan name or a range of vlanids to compare against the packet. The range is specified as vlanid/mask. For example if you specify "3200/8" then the vlanid range will be 3200-3327.

See Also

edit, *list*, *modify*, security, *security dos*, *tmsh*

profile

Configures a DoS profile.

Syntax

Configure the **profile** component within the **security dos** module using the syntax shown in the following sections.

Create/Modify

```
create profile [name]
modify profile [name]
    app-service [[string] | none]
    application [none | add | delete | modify | replace-all-with] {
      name [string] {
          bot-defense {
            collect-stats [enabled | disabled]
            cross-domain-requests [allow-all | validate-bulk | validate-upon-request]
            external-domains [none | add | delete | replace-all-with] { [string] ... }
            grace-period [integer]
            mode [always | disabled | during-attacks]
            site-domains [none | add | delete | replace-all-with] { [string] ... }
            url-whitelist [none | add | delete | replace-all-with] { [string] ... }
          }
          captcha-response {
            failure {
               body [string]
               type [custom | default]
            }
            first {
               body [string]
               type [custom | default]
            }
          }
          geolocations [none | add | delete | modify | replace-all-with] {
              [black-listed | white-listed]
          }
          heavy-urls {
            automatic-detection [enabled | disabled]
            exclude [none | add | delete | replace-all-with] { [string] ... }
            include [none | add | delete | replace-all-with] { [string] ... }
            latency-threshold [integer]
            protection [enabled | disabled]
          }
          ip-whitelist [none | add | delete | modify | replace-all-with] {
            [address ... | address/mask ... ]
          }
          latency-based {
            de-escalation-period [integer]
            escalation-period [integer]
            geo-captcha-challenge [enabled | disabled]
            geo-client-side-defense [enabled | disabled]
            geo-minimum-share [integer]
            geo-rate-limiting [enabled | disabled]
            geo-request-blocking-mode [block-all | rate-limit]
            geo-share-increase-rate [integer]
```

```
  ip-captcha-challenge [enabled | disabled]
  ip-client-side-defense [enabled | disabled]
  ip-maximum-tps [integer]
  ip-minimum-tps [integer]
  ip-rate-limiting [enabled | disabled]
  ip-request-blocking-mode [block-all | rate-limit]
  ip-tps-increase-rate [integer]
  latency-increase-rate [integer]
  maximum-latency [integer]
  minimum-latency [integer]
  mode [off | transparent | blocking]
  site-captcha-challenge [enabled | disabled]
  site-client-side-defense [enabled | disabled]
  site-maximum-tps [integer]
  site-minimum-tps [integer]
  site-rate-limiting [enabled | disabled]
  site-tps-increase-rate [integer]
  static-url-mitigation [enabled | disabled]
  url-captcha-challenge [enabled | disabled]
  url-client-side-defense [enabled | disabled]
  url-maximum-tps [integer]
  url-minimum-tps [integer]
  url-rate-limiting [enabled | disabled]
  url-tps-increase-rate [integer]
}
tcp-dump {
  maximum-duration [integer]
  maximum-size [integer]
  record-traffic [enabled | disabled]
  repetition-interval [[integer] | once-per-attack]
}
tps-based {
  de-escalation-period [integer]
  escalation-period [integer]
  geo-captcha-challenge [enabled | disabled]
  geo-client-side-defense [enabled | disabled]
  geo-minimum-share [integer]
  geo-rate-limiting [enabled | disabled]
  geo-request-blocking-mode [block-all | rate-limit]
  geo-share-increase-rate [integer]
  ip-captcha-challenge [enabled | disabled]
  ip-client-side-defense [enabled | disabled]
  ip-maximum-tps [integer]
  ip-minimum-tps [integer]
  ip-rate-limiting [enabled | disabled]
  ip-request-blocking-mode [block-all | rate-limit]
  ip-tps-increase-rate [integer]
  mode [off | transparent | blocking]
  site-captcha-challenge [enabled | disabled]
  site-client-side-defense [enabled | disabled]
  site-maximum-tps [integer]
  site-minimum-tps [integer]
  site-rate-limiting [enabled | disabled]
  site-tps-increase-rate [integer]
  static-url-mitigation [enabled | disabled]
  url-captcha-challenge [enabled | disabled]
  url-client-side-defense [enabled | disabled]
  url-maximum-tps [integer]
  url-minimum-tps [integer]
  url-rate-limiting [enabled | disabled]
  url-tps-increase-rate [integer]
}
```

```
          trigger-irule [enabled | disabled]
      }
    }
    description [string]
    dos-network [none | add | delete | modify | replace-all-with] {
      name [string] {
          behavioral-analysis [disabled | enabled]
          network-attack-vector [none | add | delete | modify | replace-all-with] {
            attack-type [ext-hdr-too-large | hop-cnt-low | host-unreachable |
icmpv4-flood | icmpv6-flood | icmp-frag | ip-frag-flood | ip-opt-frames |
ipv6-ext-hdr-frames | ipv6-frag-flood | opt-present-with-illegal-len |
tcp-opt-overruns-tcp-hdr | tcp-rst-flood | tcp-syn-flood | tcp-synack-flood | tidcmp |
too-many-ext-hdrs | udp-flood | unk-tcp-opt-type]
              rate-increase [integer]
              rate-limit [integer]
              rate-threshold [integer]
          }
      }
    }
    protocol-dns [none | add | delete | modify | replace-all-with] {
      name [string] {
          dns-query-vector [none | add | delete | modify | replace-all-with] {
            query-type [a | aaaa | any | axfr | cname | ixfr | mx | ns | other | ptr |
soa | srv | txt]
              rate-increase [integer]
              rate-limit [integer]
              rate-threshold [intege]
          }
          prot-err-attack-detection [integer]
          prot-err-atck-rate-incr [integer]
      }
    }
    protocol-sip [none | add | delete | modify | replace-all-with] {
      name [string] {
          prot-err-atck-rate-increase [integer]
          prot-err-atck-rate-threshold [integer]
          prot-err-attack-detection [integer]
          sip-method-vector [none | add | delete | modify | replace-all-with] {
            method-type [ack | cancel | message | options | prack | register | bye |
invite | notify | other | publish | subscribe]
              rate-increase [integer]
              rate-limit [integer]
              rate-threshold [integer]
          }
      }
    }
edit profile [ [ [name] | [glob] | [regex] ] ... ]
    all-properties
    non-default-properties
```

Display

```
list profile
list profile [ [ [name] | [glob] | [regex] ] ... ]
show running-config profile
show running-config profile [ [ [name] | [glob] | [regex] ] ... ]
    all-properties
    non-default-properties
    one-line
    partition
    recursive
```

Delete

```
delete profile [name]
```

Description

You can use the **profile** component to create, modify, display, or delete a DoS profile for use with DoS Protection functionality.

Examples

create profile my_dos_profile

Creates a custom DoS profile named **my_dos_profile** with initial settings.

list profile

Displays the properties of all DoS profiles.

Options

- **app-service**
  Specifies the name of the application service to which the profile belongs. The default value is **none**. **Note:** If the **strict-updates** option is **enabled** on the application service that owns the object, you cannot modify or delete the profile. Only the application service can modify or delete the profile.
- **application**
  Adds, deletes, or replaces a single Application Security sub-profile. You can configure the following options for Application Security:
  - **bot-defense**
    Specifies properties of proactive bot defense in Application Security. You can configure the following options for Proactive Bot Defense:
    - **collect-stats**
      Enables or disables domain statistics collection.
    - **cross-domain-requests**
      Specifies a cross-domain requests handling mode. The options are:
    - **allow-all**
      Allows all cross-domain requests. This is the default value.
    - **validate-bulk**
      System validates domains in bulk: the cookies for the related domains are created together with the cookie for the current domain, by generating challenges in iframes - one per each domain.
    - **validate-upon-request**
      System validates domains upon request: the cookie for the related domain is generated when a request arrives to an unqualified URL without a cookie.

- **external-domains**
  Configures a list of external domains that are allowed to link to resources of this website.
- **grace-period**
  Specifies the length of grace period (in seconds) in which only the Simple Bot Prevention is enforced.
- **mode**
  Specifies a mode of proactive bot defense. The options are:
- **always**
  Specifies that the proactive bot defense is always enabled.
- **disabled**
  Specifies that the proactive bot defense is disabled. This is the default value.
- **during-attacks**
  Specifies that the proactive bot defense is enabled only during attacks.
- **site-domains**
  Configures a list of domains that are part of the website.
- **url-whitelist**
  Configures a list of URLs to exclude from the proactive bot defense.

- **captcha-response**
  Specifies properties of the CAPTCHA response in Application Security. You can configure the following options for CAPTCHA Response Settings:
  - **failure**
    Specifies properties of a failed CAPTCHA response. You can configure the following options for a failed CAPTCHA response:
  - **body**
    Configures a failed CAPTCHA response body.
  - **type**
    Configures a type of a failed CAPTCHA response body. You can configure the following options for a failed CAPTCHA response type:
  - **custom**
    Configures a custom failed CAPTCHA response type.
  - **default**
    Configures a default failed CAPTCHA response type.
  - **first**
    Specifies properties of the first CAPTCHA response. You can configure the following options for the first CAPTCHA response:
  - **body**
    Configures the first CAPTCHA response body.

- **type**
  Configures a type of the first CAPTCHA response body. You can configure the following options for the first CAPTCHA response type:
  - **custom**
    Configures a custom first CAPTCHA response type.
  - **default**
    Configures a default first CAPTCHA response type.
- **geolocations**
  Configures a list of blacklisted/whitelisted Geolocations. You can configure the following options for each Geolocation:
  - **[black-listed | white-listed]**
    Specifies a type of Geolocation.
- **heavy-urls**
  Specifies heavy URL protection in Application Security. You can configure the following options for heavy URL protection:
  - **automatic-detection**
    Enables or disables automatic heavy URL detection. In order to enable it, you must first enable **protection**.
  - **exclude**
    Configures a list of URLs (or wildcards) to exclude from the heavy URLs.
  - **include**
    Configures a list of URLs to include in the heavy URLs.
  - **latency-threshold**
    Specifies the latency threshold for automatic heavy URL detection (in milliseconds).
  - **protection**
    Enables or disables heavy URL protection. To enable it, you must additionally enable one of the following DoS URL-based prevention policy methods: **url-client-side-defense** or **url-rate-limiting**. This can be done for either **tps-based** or **latency-based** anomaly protection.
- **ip-whitelist**
  Adds, deletes, or replaces a set of IP addresses and subnets in the whitelist of Application Security.
- **name**
  Specifies a dummy name for enabled Application Security. This option is required for the operations **create**, **delete**, **modify**, and **replace-all-with**.
- **latency-based**
  Specifies Latency-based anomaly in Application Security. You can configure the following options for Latency-based anomaly:
  - **de-escalation-period**
    Specifies the de-escalation period (in seconds) in Latency-based anomaly.

- **escalation-period**
  Specifies the escalation period (in seconds) in Latency-based anomaly.
- **geo-captcha-challenge**
  Enables or disables Geolocation-based CAPTCHA challenge in Latency-based anomaly.
- **geo-client-side-defense**
  Enables or disables Geolocation-based client side integrity defense in Latency-based anomaly.
- **geo-minimum-share**
  Specifies the minimum traffic share for detection in Geolocation detection criteria of Latency-based anomaly.
- **geo-rate-limiting**
  Enables or disables Geolocation-based rate limiting in Latency-based anomaly.
- **geo-request-blocking-mode**
  Specifies a Geolocation-based request blocking mode of Latency-based anomaly. The options are:
- **block-all**
  Specifies that the system blocks all requests from the respective Geolocation.
- **rate-limit**
  Specifies that the system blocks requests from the respective Geolocation based on the traffic share ratio. This is the default value.
- **geo-share-increase-rate**
  Specifies the percentage by which TPS increased in Geolocation detection criteria of Latency-based anomaly.
- **ip-captcha-challenge**
  Enables or disables Source IP-based CAPTCHA challenge in Latency-based anomaly.
- **ip-client-side-defense**
  Enables or disables Source IP-based client side integrity defense in Latency-based anomaly.
- **ip-maximum-tps**
  Specifies the amount which TPS reached in IP detection criteria of Latency-based anomaly.
- **ip-minimum-tps**
  Specifies the minimum TPS threshold for detection in IP detection criteria of Latency-based anomaly.
- **ip-rate-limiting**
  Enables or disables Source IP-based rate limiting in Latency-based anomaly.
- **ip-request-blocking-mode**
  Specifies a Source IP-based request blocking mode of Latency-based anomaly. The options are:

- **block-all**
  Specifies that the system blocks all requests from the respective Source IP address.
- **rate-limit**
  Specifies that the system blocks requests from the respective Source IP address based on the traffic share ratio. This is the default value.
- **ip-tps-increase-rate**
  Specifies the percentage by which TPS increased in IP detection criteria of Latency-based anomaly.
- **latency-increase-rate**
  Specifies the percentage by which latency increased in detection criteria of Latency-based anomaly.
- **maximum-latency**
  Specifies the amount which latency reached (in milliseconds) in detection criteria of Latency-based anomaly.
- **minimum-latency**
  Specifies the minimum latency threshold for detection (in milliseconds) in detection criteria Latency-based anomaly.
- **mode**
  Specifies an operation mode of Latency-based anomaly. The options are:
- **off**
  Specifies that the system does not check for DoS attacks. This is the default value.
- **transparent**
  Specifies that when the system detects an attack, it displays the attack data on the Reporting DoS Attacks screen. In transparent mode the system does not drop requests either from the attacking IP address, or to attacked URLs.
- **blocking**
  Specifies that when the system detects an attack, in addition to displaying the attack data on the Reporting DoS Attacks screen, the system also drops either connections from the attacking IP address, or requests to attacked URLs.
- **site-captcha-challenge**
  Enables or disables Site-wide CAPTCHA challenge in Latency-based anomaly.
- **site-client-side-defense**
  Enables or disables Site-wide client side integrity defense in Latency-based anomaly.
- **site-maximum-tps**
  Specifies the amount which TPS reached in Site-wide detection criteria of Latency-based anomaly.
- **site-minimum-tps**
  Specifies the minimum TPS threshold for detection in Site-wide detection criteria of Latency-based anomaly.

- **site-rate-limiting**
  Enables or disables Site-wide rate limiting in Latency-based anomaly.
- **site-tps-increase-rate**
  Specifies the percentage by which TPS increased in Site-wide detection criteria of Latency-based anomaly.
- **static-url-mitigation**
  Enables or disables Static URL mitigation in Latency-based anomaly.
- **url-captcha-challenge**
  Enables or disables URL-based CAPTCHA challenge in Latency-based anomaly.
- **url-client-side-defense**
  Enables or disables URL-based client side integrity defense in Latency-based anomaly.
- **url-maximum-tps**
  Specifies the amount which TPS reached in URL detection criteria of Latency-based anomaly.
- **url-minimum-tps**
  Specifies the minimum TPS threshold for detection in URL detection criteria of Latency-based anomaly.
- **url-rate-limiting**
  Enables or disables URL-based rate limiting in Latency-based anomaly.
- **url-tps-increase-rate**
  Specifies the percentage by which TPS increased in URL detection criteria of Latency-based anomaly.

- **tcp-dump**
  Specifies properties of traffic recording during attacks in Application Security. You can configure the following options for Record Traffic During Attacks:
  - **maximum-duration**
    Specifies the TCP dump maximum duration (in seconds).
  - **maximum-size**
    Specifies the TCP dump maximum size (in megabytes).
  - **record-traffic**
    Enables or disables traffic recording during attacks.
  - **repetition-interval**
    Specifies the TCP dump repetition interval (in seconds).
- **tps-based**
  Specifies TPS-based anomaly in Application Security. You can configure the following options for TPS-based anomaly:
  - **de-escalation-period**
    Specifies the de-escalation period (in seconds) in TPS-based anomaly.

- **escalation-period**
  Specifies the escalation period (in seconds) in TPS-based anomaly.
- **geo-captcha-challenge**
  Enables or disables Geolocation-based CAPTCHA challenge in TPS-based anomaly.
- **geo-client-side-defense**
  Enables or disables Geolocation-based client side integrity defense in TPS-based anomaly.
- **geo-minimum-share**
  Specifies the minimum traffic share for detection in Geolocation detection criteria of TPS-based anomaly.
- **geo-rate-limiting**
  Enables or disables Geolocation-based rate limiting in TPS-based anomaly.
- **geo-request-blocking-mode**
  Specifies a Geolocation-based request blocking mode of TPS-based anomaly. The options are:
- **block-all**
  Specifies that the system blocks all requests from the respective Geolocation.
- **rate-limit**
  Specifies that the system blocks requests from the respective Geolocation based on the traffic share ratio. This is the default value.
- **geo-share-increase-rate**
  Specifies the percentage by which TPS increased in Geolocation detection criteria of TPS-based anomaly.
- **ip-captcha-challenge**
  Enables or disables Source IP-based CAPTCHA challenge in TPS-based anomaly.
- **ip-client-side-defense**
  Enables or disables Source IP-based client side integrity defense in TPS-based anomaly.
- **ip-maximum-tps**
  Specifies the amount which TPS reached in IP detection criteria of TPS-based anomaly.
- **ip-minimum-tps**
  Specifies the minimum TPS threshold for detection in IP detection criteria of TPS-based anomaly.
- **ip-rate-limiting**
  Enables or disables Source IP-based rate limiting in TPS-based anomaly.
- **ip-request-blocking-mode**
  Specifies a Source IP-based request blocking mode of TPS-based anomaly. The options are:

- **block-all**
  Specifies that the system blocks all requests from the respective Source IP address.
- **rate-limit**
  Specifies that the system blocks requests from the respective Source IP address based on the traffic share ratio. This is the default value.
- **ip-tps-increase-rate**
  Specifies the percentage by which TPS increased in IP detection criteria of TPS-based anomaly.
- **mode**
  Specifies an operation mode of TPS-based anomaly. The options are:
- **off**
  Specifies that the system does not check for DoS attacks. This is the default value.
- **transparent**
  Specifies that when the system detects an attack, it displays the attack data on the Reporting DoS Attacks screen. In transparent mode the system does not drop requests either from the attacking IP address, or to attacked URLs.
- **blocking**
  Specifies that when the system detects an attack, in addition to displaying the attack data on the Reporting DoS Attacks screen, the system also drops either connections from the attacking IP address, or requests to attacked URLs.
- **site-captcha-challenge**
  Enables or disables Site-wide CAPTCHA challenge in TPS-based anomaly.
- **site-client-side-defense**
  Enables or disables Site-wide client side integrity defense in TPS-based anomaly.
- **site-maximum-tps**
  Specifies the amount which TPS reached in Site-wide detection criteria of TPS-based anomaly.
- **site-minimum-tps**
  Specifies the minimum TPS threshold for detection in Site-wide detection criteria of TPS-based anomaly.
- **site-rate-limiting**
  Enables or disables Site-wide rate limiting in TPS-based anomaly.
- **site-tps-increase-rate**
  Specifies the percentage by which TPS increased in Site-wide detection criteria of TPS-based anomaly.
- **static-url-mitigation**
  Enables or disables Static URL mitigation in TPS-based anomaly.

- **url-captcha-challenge**
  Enables or disables URL-based CAPTCHA challenge in TPS-based anomaly.
- **url-client-side-defense**
  Enables or disables URL-based client side integrity defense in TPS-based anomaly.
- **url-maximum-tps**
  Specifies the amount which TPS reached in URL detection criteria of TPS-based anomaly.
- **url-minimum-tps**
  Specifies the minimum TPS threshold for detection in URL detection criteria of TPS-based anomaly.
- **url-rate-limiting**
  Enables or disables URL-based rate limiting in TPS-based anomaly.
- **url-tps-increase-rate**
  Specifies the percentage by which TPS increased in URL detection criteria of TPS-based anomaly.

- **trigger-irule**
  Specifies, when **enabled**, that the system activates an Application DoS iRule event. The default value is **disabled**.

◆ **description**
User defined description.

◆ **protocol-dns**
Adds, deletes, or replaces a single Protocol DNS Security sub-profile. You can configure the following options for Protocol DNS Security:

- **name**
  Specifies a dummy name for enabled Protocol DNS Security. This option is required for the operations **create**, **delete**, **modify**, and **replace-all-with**.
- **dns-query-vector**
  Adds, deletes, or replaces Protocol DNS DoS vectors. You can configure the following options for DNS query vectors:
  - **query-type**
    Specifies the vector (DNS query) type for DoS attack detection.
  - **rate-increase**
    Specifies the rate increase for DoS attack detection.
  - **rate-limit**
    Specifies the rate limit for DoS attack detection.
  - **rate-threshold**
    Specifies the rate threshold for DoS attack detection.
- **prot-err-attack-detection**
  Specifies if protocol errors attack detection is enabled or not. Eg: Malformed, Malicious DoS attacks.
- **prot-err-atck-rate-incr**
  Specifies the protocol errors rate increase for DoS attack detection.

- **rate-limit**
  Specifies the protocol errors rate limit for DoS attack detection.
- **rate-threshold**
  Specifies the protocol errors rate threshold for DoS attack detection.

◆ **protocol-sip**
Adds, deletes, or replaces a single Protocol SIP Security sub-profile. You can configure the following options for Protocol SIP Security:

- **name**
  Specifies a dummy name for enabled Protocol SIP Security. This option is required for the operations **create**, **delete**, **modify**, and **replace-all-with**.
- **prot-err-atck-rate-increase**
  Specifies the protocol errors rate increase for DoS attack detection.
- **prot-err-atck-rate-threshold**
  Specifies the protocol errors rate threshold for DoS attack detection.
- **prot-err-attack-detection**
  Specifies if protocol errors attack detection is enabled or not. Eg: Malformed packets DoS attacks.
- **sip-method-vector**
  Adds, deletes, or replaces Protocol SIP DoS vectors. You can configure the following options for SIP method vectors:
  - **method-type**
    Specifies the vector type (SIP method) for DoS attack detection.
  - **rate-increase**
    Specifies the rate increase for DoS attack detection.
  - **rate-limit**
    Specifies the rate limit for DoS attack detection.
  - **rate-threshold**
    Specifies the rate threshold for DoS attack detection.
- **dos-network**
  Adds, deletes, or replaces a single Network DoS Security sub-profile. You can configure the following options for Network DoS Security:
  - **name**
    Specifies a dummy name for enabled Network DoS Security. This option is required for the operations **create**, **delete**, **modify**, and **replace-all-with**.
  - **behavioral-analysis**
    This setting can be used to enable or disable the Behavioral based Anomaly/DoS feature per virtual server by associating this profile to that virtual server. Default is disabled.
  - **network-attack-vector**
    Adds, deletes, or replaces Network Attack DoS vectors. You can configure the following options for Network Attack vectors:
  - **attack-type**
    Specifies the vector type (Network Attack) for DoS attack detection.

  - **rate-increase**
    Specifies the rate increase for DoS attack detection.
  - **rate-limit**
    Specifies the rate limit for DoS attack detection.
  - **rate-threshold**
    Specifies the rate threshold for DoS attack detection.
- **glob**
  Displays the items that match the **glob** expression. See **help glob** for a description of **glob** expression syntax.
- **name**
  Specifies a unique name for the component. This option is required for the commands **create**, **delete**, and **modify**.
- **partition**
  Displays the administrative partition within which the component resides.
- **regex**
  Displays the items that match the regular expression. The regular expression must be preceded by an at sign (@[regular expression]) to indicate that the identifier is a regular expression. See **help regex** for a description of regular expression syntax.

See Also

create, *delete*, *edit*, glob, *list*, *virtual*, *modify*, regex, security, *security dos*, *show*, *tmsh*

udp-portlist

Configures the DoS udp portlist component within the **security dos** module using the syntax shown in the following sections. These DoS udp portlist entries are applied to all udp packets except those going through the management interface.

Syntax

Modify

```
modify udp-portlist dos-udp-portlist
  description [string]
  list-type [exclude-listed-ports | include-listed-ports]
  entries [modify | replace-all-with] {
     [entry] {
        description [string]
        match-direction [both | dst | none | src]
        port-number [number]
     }
  }
```

Display

```
list udp-portlist
```

Description

You can use the **udp-portlist** component to configure a DoS UDP portlist of upto eight entries for all UDP traffic except the management interface. The HSB hardware compares all incoming UDP traffic to the **udp-portlist** entries. There are 2 types of behavior, depending upon whether the udp port list is configured as a white list or as a black list. White list and black list are mutually exclusive properties of a UDP port list.

If the udp port list is configured as a **list-type** of **exclude-listed-ports**, and if a match is found on an incoming packet, then we do not increment the UDP Flood DoS vector. If a match is not found, then the UDP Flood DoS vector checks are done on those packets.

If the udp port list is configured as a **list-type** of **include-listed-ports**, and if a match is found on an incoming packet, then we increment the UDP Flood DoS vector. If a match is not found, then the UDP Flood DoS vector checks are not done on the packets.

Either destination port or source port or both can be specified in a udp-portlist entry.

Examples

modify udp-portlist dos-udp-portlist description "bad ports" list-type include-listed-ports Modifies the udp-portlist dos-udp-portlist to a blacklist.

modify udp-portlist dos-udp-portlist list-type exclude-listed-ports Modifies the udp-portlist dos-udp-portlist to a white-list.

modify udp-portlist dos-udp-portlist description "bad ports" entries modify { entry1 { match-direction src port-number 161 } }Modifies an entry. The new entry is for source UDP port 161. It matches any UDP packet whose source port is 161.

modify udp-portlist dos-udp-portlist entries modifiy { 161 { match-direction both } }

Modifies the entry for destination UDP port 161 to source and destination port 161. It matches
any UDP packet whose destination or source port is 161.

```
security dos udp-portlist dos-udp-portlist {
   entries {
       entry1 {
           match-direction both
           port-number snmp
       }
       entry2 { }
       entry3 { }
       entry4 { }
   }
   white-list
}
```

Displays the current list of DoS UDP portlist entries.

Options

- **description**
  Your description for the DoS **udp-portlist**.
- **list-type**
  Sets the list type to be either exclude-listed-ports or include-listed-ports
  - **include-listed-ports**
    Sets the property of the dos-udp-portlist list to include-listed-ports (Blacklist).
  - **exclude-listed-ports**
    Sets the property of the dos-udp-portlist list to exclude-listed-ports (Whitelist).
- **entries**
  Modifies a **udp-portlist** entry.
  - **modify**
    Modifies the existing entry that you specify next, in curly braces ({}). After the entry name, enter the new configuration (port mode and port number) settings for the entry inside a nested set of curly braces.

- **replace-all-with**
  Replaces the current set of **udp-portlist** entries with the entry(s) that you specify next, in curly braces ({}).

Enter the name of a entry to be modified, then enter an open curly brace ({), one or more of the following options, and a closed curly brace (}).

- **description**
  Your description for the current entry.
- **match-direction**
  Set the mode of matching (source, destination or both).
- **port-number**
  Set the port number for matching.

See Also

edit, *list*, *modify*, security, *security dos*, *tmsh*

85

security firewall

- Introducing the security firewall module
- Alphabetical list of components

Introducing the security firewall module

You can use the tmsh components that reside within the security firewall module to create firewall rules. For more information about the tmsh hierarchical structure, see Chapter 2, *Understanding and Using the Traffic Management Shell*.

Alphabetical list of components

The remainder of this chapter lists the tmsh components that are available in the security firewall module.

address-list

Configures an address-list for use by firewall rules. An *address list* is a list of IP-address prefixes to compare against the source-IP address and/or destination-IP address in an IP packet.

Syntax

Create/Modify

```
create address-list [name]
modify address-list [[name] | all]
  addresses [add | delete | modify | replace-all-with] {
   [ [ip address] ]
  }
  app-service [name]
  description [string]
edit address-list [[name] | all]
    all-properties
    non-default-properties
```

Display

```
list address-list [[name] | all | [property]]
show running-config address-list [[name] | all | [property]]
```

Delete

```
delete address-list [[name] | all]
```

Description

You can use the **address-list** component to define reusable lists of addresses. You can use an address list in any of the following firewalls and firewall rule lists: **net self**, **net route-domain**, **security firewall global-rules**, **security firewall rule-list**, **security firewall management-ip-rules**, and **ltm virtual**. A firewall rule compares all of the addresses in the list to either the source or destination IP in the packet, depending on how you apply the list. If there is a match, the firewall rule takes an action, such as accepting or dropping the packet.

Examples

create address-list alist1 addresses add { 10.10.1.1 10.10.1.2 192.168.24.0/24 }

Creates a new address list, "alist1," with two IPv4 addresses and one IPv4 subnet.

modify address-list alist1 addresses modify { 10.10.1.1 { description "management IP at wwmed site3" } }

Modifies the above address list with a description for the first address.

modify address-list alist1 addresses add { 2001:DB8:a::/64 }

Modifies the same address list by adding an IPv6 subnet.

```
list address-list alist1
security firewall address-list alist1 {
   addresses {
       10.10.1.1 {
           description "management IP at wwmed site3"
       }
       10.10.1.2 { }
       192.168.24.0/24 { }
       2001:db8:a::/64 { }
   }
}
```

Shows the modified address list.

Options

- **addresses**
  Specifies a list of IP addresses and/or subnets to compare against a packet's source or destination address. The format for an IPv4 address is *a*. *b*. *c*. *d* [/ *prefix*]. The general format for an IPv6 address is *a*: *b*: *c*: *d*: *e*: *f*: *g*: *h* [/ *prefix*]; you can shorten this by eliminating leading zeros from each field (for example, you can shorten "2001:0db7:3f4a:09dd:ca90:ff00:0042:8329" to "2001:db7:3f4a:9dd:ca90:ff00:42:8329"), and/or by removing the longest contiguous field of zeros (for example, you can shorten "2001:0:0:0:c34a:0:23ff:678" to "2001::c34a:0:23ff:678"). TMSH accepts any valid text representation of IPv6 addresses, as defined in RFC 2373 (see http://www.ietf.org/rfc/rfc2373.txt).
  The next keyword specifies the action to take with the addresses (add, delete, modify, or replace the current set of addresses).
  - **add**
    Creates a new address list, which you specify next with IP addresses and/or prefixes in curly braces ({}).
  - **delete**
    Deletes the address(es) that you specify next, in curly braces ({}).
  - **modify**
    Makes it possible to replace the optional description(s) for the address(es). You can specify a description in a nested set of curly braces after each address.
  - **replace-all-with**
    Replaces the current set of IP addresses with the address(es) that you specify next, in curly braces ({}).
- **app-service**
  Associates this address list with a particular Application Service. An *Application Service* is a major component of an iApp, an advanced

configuration tool for creating and maintaining similar applications on multiple servers. The **asm** module (see *asm*) has components for working with iApps.

- **description**
  Is your description for this address list.

See Also

edit, *list*, *modify*, *self*, *route-domain*, *global-rules*, *management-ip-rules*, *rule-list*, *virtual*, *tmsh*

global-rules

Configures the global network firewall rules. These firewall rules are applied to all packets except those going through the management interface. They are applied first, before any firewall rules for the packet's virtual server, route domain, and/or self IP.

Syntax

Modify

```
modify global-rules
  description [string]
  enforced-policy [ [policy_name] | none ]
  rules [add | delete | modify | replace-all-with] {
     [ [name] ] {
        action [accept | accept-decisively | drop | reject]
        app-service [name]
        description [string]
        destination {
          address-lists [add | default | delete | replace-all-with] {
            [address list names...]
          }
          address-lists none
          addresses [add | default | delete | replace-all-with] {
            [ [ip address] | [ip address/prefixlen] ]
          }
          addresses none
          geo [add | default | delete | replace-all-with] {
            [ [country_code [state state_name] ] ]
          }
          geo none
          port-lists [add | default | delete | replace-all-with] {
            [port list names...]
          }
          port-lists none
          ports [add | default | delete | none | replace-all-with] {
            [ [port] | [port1-port2] ]
          }
          ports none
        }
        icmp [add | delete | modify | replace-all-with] {
          [ [icmp_type] | icmp_type:icmp_code ] {
            description [string]
          }
        }
        icmp none
        ip-protocol [protocol name]
        irule [irule name]
        irule-sample-rate [integer]
        log [no | yes]
        place-after [first | last | [rule name]]
        place-before [first | last | [rule name]]
        rule-list [rule list name]
        schedule [schedule name]
        source {
          address-lists [add | default | delete | replace-all-with] {
```

```
            [address list names...]
          }
          address-lists none
          addresses [add | default | delete | replace-all-with] {
            [ [ip address] | [ip_address/prefixlen] ]
          }
          addresses none
          geo [add | default | delete | replace-all-with] {
            [ [country_code [state state_name] ] ]
          }
          geo none
          port-lists [add | default | delete | replace-all-with] {
            [port list names...]
          }
          port-lists [add | default | delete | replace-all-with] {
            [port list names...]
          }
          port-lists none
          ports [add | default | delete | replace-all-with] {
            [ [port] | [port1-port2] ]
          }
          ports none
          vlans [add | default | delete | replace-all-with] {
            [vlan names...]
          }
          vlans none
        }
        status [disabled | enabled | scheduled]
      }
    }
    rules none
    staged-policy [ [policy_name] | none ]
edit global-rules
    all-properties
    non-default-properties
reset-stats virtual [ [ [name] | [glob] | [regex] ] ... ]
  enforced-policy-rules { [rule name] }
  rules  { [rule name] }
  staged-policy-rules  { [rule name] }
```

Display

```
list global-rules
show running-config global-rules
```

Description

You can use the **global-rules** component to configure network firewall rules for all traffic except the management interface. The network software compares IP packets to the criteria specified in these rules. If a packet matches the criteria, then the system takes the action specified by the rule (such as accepting or dropping the packet). If a packet does not match a global rule, the network software either accepts the packet or passes it to the next set of rules (for example, the system compares the packet to **net route-domain** rules if the packet is destined for a **route-domain** that has firewall rules defined).

Matching An Ip Packet

You can use this TMSH component to match against any or all of the following properties of an IP packet:

- source address
- source geo
- source port
- the packet's source VLAN
- destination address
- destination geo
- destination port
- the higher-level protocol in the packet's payload

If you match against more than one of these items, a packet must pass *all* of your tests to successfully match. For example, if you match against a source subnet and several destination ports, a packet must originate from the given subnet and must also have one of the specified destination ports.

Rule Order

The network software evaluates firewall rules in the order that you specify. You can use the **list global-rules** command to see the current rule order. As you add or modify rules in this component, you can use the **place-before** *rule-name* or **place-after** *rule-name* option to choose the rule's place in the sequence.

Rule order can determine whether or not a packet is dropped. Consider the following rules:

- rule_a, matches source addresses against 172.16.0.0 and ACCEPTS all packets that match.
- rule_d, matches source addresses against 172.16.39.0 and DROPS all packets that match.

Also consider a packet from a host at 172.16.39.55. If rule_a appears before rule_d in the rule list, the packet's source address matches rule_a first and the software accepts it. The software never reaches rule_d for comparison. If rule_d appears first instead, the packet's source address now matches rule_d; in this case, the software drops the packet.

Examples

modify global-rules rules add { reject-internal-net { source { addresses replace-all-with { 172.27.0.0/16 } } } action reject place-before first } }

Creates a rule entry at the beginning of the list that rejects traffic from the 172.27.0.0 network.

```
list global-rules
security firewall global-rules {
   rules {
       reject-internal-net {
           action reject
           source {
               addresses {
                   172.27.0.0/16 { }
               }
           }
       }
   }
}
security firewall global-rules {
   rules {
       r1 {
           action drop
           source {
               geo {
                   US {
                       state none
                   }
               }
           }
       }
   }
}
```

Displays the current list of global rules.

modify global-rules rules delete { reject-internal-net }

Removes the "reject-internal-net" rule from the list of global rules.

Options

- **description**
  Your description for the global list of firewall rules.
- **enforced-policy**
  Specifies an enforced firewall policy. **enforced-policy** rules are enforced globally as if the policy rules were explicitly defined in the global-rules' **rules**. Either **rules** or **enforced-policy** can be configured in global-rules, not both of them.
- **enforced-policy-rules**
  Specifies firewall rules enforced on traffic globally via referenced **enforced-policy**.
- **rules**
  Adds, deletes, or replaces a firewall rule.

- **add**
  Creates a new rule, which you specify next with a unique string in curly braces ({}). Use the **place-before** or **place-after** option inside the curly braces to determine the order of the rule. If this is the first rule, use **place-before first**.
- **delete**
  Deletes the rule that you specify next, in curly braces ({}). You can use **delete {all}** to empty the list of firewall rules, which has the same effect as using **none** (see below).
- **modify**
  Modifies the existing rule that you specify next, in curly braces ({}). After the rule name, enter the new configuration settings for the rule inside a nested set of curly braces.
- **replace-all-with**
  Replaces the current set of global rules with the rule(s) that you specify next, in curly braces ({}). You can use this option for the first global rule.
- **none**
  Empties the list of global rules. The security software skips this context and assesses packets against the next layer of firewall rules (such as those defined for **net route-domain**, **net self-ip**, or **ltm virtual**)

Enter the name of a rule to be added or modified, then enter an open curly brace ({), one or more of the following options, and a closed curly brace (}).

- **action**
  Specifies the action that the system takes when a packet matches the rule.
  - **accept**
    Specifies that a matching packet should be accepted. The security software stops comparing a matching packet to any other global rules. The software continues comparing the packet to rules in the next appropriate context (such as **net self-ip**, **net route-domain** or **ltm virtual**).
  - **accept-decisively**
    Specifies that a matching packet should be accepted and should not be compared to any other firewall rules in any other context.
  - **drop**
    Specifies that a matching packet should be silently dropped. The security software sends nothing back to the packet source. The security software does not compare the packet to any other firewall rules in any other context.
  - **reject**
    Specifies that a matching packet should be dropped. For TCP-based protocols, the security software sends a TCP reset (with the RST flag raised) back to the source. For other protocols, **reject** is equivalent to **drop**.

- **app-service**
  Associates the global-rule list with a particular Application Service. An *Application Service* is a major component of an iApp, an advanced configuration tool for creating and maintaining similar applications on multiple servers. The *asm* module has components for working with iApps.
- **description**
  Your description for the current rule.
- **destination**
  Matches against each packet's destination IP and/or destination port. The next options choose the matching criteria.
  - **address-lists**
    Specifies a list of IP-address lists (see *address-list*) to compare against the packet's destination address.
    This list uses the same **add**, **delete**, **none**, and **replace-all-with** options described above for rules, as well as a **default** option.
  - **addresses**
    Specifies a list of IP addresses and networks to compare against the packet's destination address.
    The format for an IPv4 address is *a*. *b*. *c*. *d* [/ *prefix*]. The general format for an IPv6 address is *a*: *b*: *c*: *d*: *e*: *f*: *g*: *h* [/ *prefix*]; you can shorten this by eliminating leading zeros from each field (for example, you can shorten "2001:0db7:3f4a:09dd:ca90:ff00:0042:8329" to "2001:db7:3f4a:9dd:ca90:ff00:42:8329"), and/or by removing the longest contiguous field of zeros (for example, you can shorten "2001:0:0:0:c34a:0:23ff:678" to "2001::c34a:0:23ff:678"). TMSH accepts any valid text representation of IPv6 addresses, as defined in RFC 2373 (see http://www.ietf.org/rfc/rfc2373.txt).
    To edit this list, use the same **add**, **delete**, **modify**, **none**, and **replace-all-with** options described above for rules.
  - **geo**
    Specifies a list of Geo Locations to compare a packet's source or destination Geo Location.
    The format for a Geo Location is a 2 character string for the country code and a string for the state.
    To edit this list, use the same **add**, **delete**, **modify**, **none**, and **replace-all-with** options described above for rules.
  - **port-lists**
    Specifies a collection of port lists (see *port-list*) to compare against the packet's destination port. If you use this option to specify a port list, a packet only matches if its destination port matches a port on these lists.
    This list uses the same **add**, **delete**, **none**, and **replace-all-with** optionss described above for rules, as well as a **default** option.

- **ports**
  Specifies one list of ports and port ranges to compare against the packet's destination port.
  To edit this list, use the same **add**, **delete**, **modify**, **none**, and **replace-all-with** options described above for rules.

- **icmp**
  Specifies a list of ICMP types and codes to compare against the packet. You must set the **ip-protocol** option to "icmp" for this option to function. If you use this option, the current rule only matches ICMP packets that have the ICMP properties you specify here. You can **add**, **delete**, or **modify** (that is, change the description of) any entry in the list, or **replace-all-with** a new set of entries that you specify between curly braces ({}).
  Use the standard integer identifiers to specify an ICMP type. For example: 3 is destination unreachable and 3:1 is destination unreachable with a code of host unreachable. The official list of ICMP types and codes is here: http://www.iana.org/assignments/icmp-parameters/icmp-parameters.xml.

- **ip-protocol**
  Specifies the IP protocol to compare against the packet. This could be a layer-3 protocol (such as ipv4 or ipv6), or a higher-level protocol like ospf or rdp. If you specify this option, a packet only matches if it uses the chosen protocol. Press the <tab> key for a full list of valid protocols.

- **irule**
  Specifies the name of the iRule that will be triggered when a packet matches this firewall rule. The firewall rule match raises a FLOW_INIT iRule event.

- **irule-sample-rate**
  Specifies the rate at which an iRule specified by **irule** option will be triggered when a packet matches this firewall rule. The rate is an integer value in the range 0-65535 and specifies how many packets must match this firewall rule before the iRule is triggered. The default value is 1 and causes the iRule to be triggered for every packet that matches this firewall rule. A value of 0 disables iRule triggering.

- **log**
  Specifies whether the security software should write a log entry for all packets that match this rule. You must also enable **network filter** logging with the *profile* component for this option to have any effect. Note that the security software always increments the statistics counter when a packet matches a rule, no matter how you set this option.

- **place-after [first | last | rule-name]**
  Specifies that a new rule should be placed after the **first** rule, the **last** rule, or the *rule-name* you specify. If you are adding individual rules (as opposed to specifying **replace-all-with**), then you must use **place-before** or **place-after** to specify the rule's position in the list.

- **place-before [first | last | rule-name]**
  Specifies that a new rule should be placed before the **first** rule, the **last** rule, or the *rule-name* you specify. If you are adding individual rules (as opposed to specifying **replace-all-with**), then you must use **place-before** or **place-after** to specify the rule's position in the list.
- **rule-list**
  Specifies a full rule list instead of a customized rule that you might define with the other options. See *rule-list*. If you use this option, then only the **schedule** and **status** options are valid; the tmsh software rejects any other options that you attempt to use with **rule-list**.
- **schedule**
  Specifies a schedule for the rule. See *schedule*. If you omit this option, the rule or rule list is enabled all the time.
  If the rule refers to a **rule-list**, the **rule-list** is enabled according to the schedule. When the **rule list** is enabled, the security software then honors the schedules defined within the **rule-list**.
- **source**
  Matches against each packet's source IP, source port, and/or source VLAN. The next options choose the matching criteria.
  - **address-lists**
    Specifies a list of address lists (see *address-list*) to compare against the packet's source address.
    This list uses the same **add**, **delete**, **none**, and **replace-all-with** options described above for rules, as well as a **default** option.
  - **addresses**
    Specifies a list of IP addresses and networks to compare against the packet's source address.
    The format for an IPv4 address is *a*. *b*. *c*. *d*. The general format for an IPv6 address is *a*: *b*: *c*: *d*: *e*: *f*: *g*: *h*.
    To edit this list, use the same **add**, **delete**, **modify**, **none**, and **replace-all-with** options described above for rules.
  - **geo**
    Specifies a list of Geo Locations to compare a packet's source or destination Geo Location.
    The format for a Geo Location is a 2 alphabet string for the country code and a string for the state.
    To edit this list, use the same **add**, **delete**, **modify**, **none**, and **replace-all-with** options described above for rules.
  - **port-lists**
    Specifies a collection of port lists (see *port-list*) to compare against the packet's source port. If you use this option to specify a port list, a packet only matches if its source port matches a port on these lists.
    If you combine address lists and port lists in the same rule, a packet must have a matching port **and** a matching address to fully match the rule.
    This list uses the same **add**, **delete**, **none**, and **replace-all-with** options described above for rules, as well as a **default** option.

- **ports**
  Specifies a list of ports and port ranges to compare against the packet's source port.
  To edit this list, use the same **add**, **delete**, **modify**, **none**, and **replace-all-with** options described above for rules.
- **vlans**
  Specifies a list of VLANs, VLAN groups, and tunnels to compare against the packet.
  This list uses the same **add**, **delete**, **none**, and **replace-all-with** options described above for rules, as well as a **default** option.

- **status**
  Specifies whether the rule is **enabled**, **disabled** or **scheduled**. A rule that is **enabled** is always checked. A rule that is **disabled** is never checked. A rule that is **scheduled** is checked according to the corresponding schedule configuration. A rule that is **scheduled** must have an associated schedule configuration.

◆ **staged-policy**
Specifies a staged firewall policy. **staged-policy** rules are not enforced while all the visibility aspects namely statistics, reporting and logging function as if the **staged-policy** rules were enforced globally.

◆ **staged-policy-rules**
Specifies firewall rules staged on traffic globally via referenced **staged-policy**.

See Also

edit, *list*, *modify*, *address-list*, *port-list*, *rule-list*, *profile*, *schedule*, *tmsh*

management-ip-rules

Configures the management IP firewall rules. These firewall rules are applied to all packets that go through the management interface.

Syntax

Modify

```
modify management-ip-rules
  description [string]
  rules [add | delete | modify | replace-all-with] {
     [ [name] ] {
        action [accept | accept-decisively | drop | reject]
        description [string]
        destination {
          address-lists [add | default | delete | replace-all-with] {
            [address list names...]
          }
          address-lists none
          addresses [add | default | delete | replace-all-with] {
            [ [ip address] | [ip address/prefixlen] ]
          }
          addresses none
          port-lists [add | default | delete | replace-all-with] {
            [port list names...]
          }
          port-lists none
          ports [add | default | delete | none | replace-all-with] {
            [ [port] | [port1-port2] ]
          }
          ports none
        }
        icmp [add | delete | modify | replace-all-with] {
          [ [icmp_type] | icmp_type:icmp_code ] {
            description [string]
          }
        }
        icmp none
        ip-protocol [protocol name]
        log [no | yes]
        place-after [first | last | [rule name]]
        place-before [first | last | [rule name]]
        rule-list [rule list name]
        schedule [schedule name]
        source {
          address-lists [add | default | delete | replace-all-with] {
            [address list names...]
          }
          address-lists none
          addresses [add | default | delete | replace-all-with] {
            [ [ip address] | [ip_address/prefixlen] ]
          }
          addresses none
          port-lists [add | default | delete | replace-all-with] {
            [port list names...]
          }
```

```
            port-lists none
            ports [add | default | delete | replace-all-with] {
              [ [port] | [port1-port2] ]
            }
            ports none
            vlans [add | default | delete | replace-all-with] {
              [vlan names...]
            }
            vlans none
          }
          status [disabled | enabled | scheduled]
        }
      }
      rules none
    edit management-ip-rules
        all-properties
        non-default-properties
```

Display

```
list management-ip-rules
show running-config management-ip-rules
```

Description

You can use the **management-ip-rules** component to configure network firewall rules that are applied to all management interface traffic. The network software compares IP packets to the criteria specified in these rules. If a packet matches the criteria then the system takes the action specified by the rule. If a packet does not match a rule then the software compares the packet against the next rule. If a packet does not match any rule the packet is accepted.

For configuration sync **management-ip-rules** are synced to the devicegroup that has a **type** field of **sync-failover**. See *config-sync*.

Matching An Ip Packet

You can use this TMSH component to match against any or all of the following properties of an IP packet:

- source address
- source port
- the packet's source VLAN
- destination address
- destination port

- the higher-level protocol in the packet's payload

If you match against more than one of these items, a packet must pass *all* of your tests to successfully match. For example, if you match against a source subnet and several destination ports, a packet must originate from the given subnet and must also have one of the specified destination ports.

Rule Order

Rules are evaluated in the order that you specify. You can use the **list management-ip-rules** command to see the current rule order. As you add or modify rules in this component, you can use the **place-before** *rule-name* or **place-after** *rule-name* option to choose the rule's place in the sequence.

Rule order can determine whether or not a packet is dropped. Consider the following rules:

- rule_a, matches source addresses against 172.16.0.0 and ACCEPTS all packets that match.

- rule_d, matches source addresses against 172.16.39.0 and DROPS all packets that match.

Also consider a packet from a host at 172.16.39.55. If rule_a appears before rule_d in the rule list, the packet's source address matches rule_a first and the software accepts it. The software never reaches rule_d for comparison. If rule_d appears first instead, the packet's source address now matches rule_d; in this case, the software drops the packet.

Examples

modify management-ip-rules rules add { reject-internal-net { source { addresses replace-all-with { 172.27.0.0/16 } } action reject place-before first } }

Creates a rule entry at the beginning of the list that rejects traffic from the 172.27.0.0 network.

modify management-ip-rules rules add { reject-insecure-ports { rule-list block_bad_mgmt place-before first } }

Adds a sub rule list to the management-IP firewall. Use the *rule-list* component to create a custom rule list.

```
list management-ip-rules
security firewall management-ip-rules {
   rules {
       reject-insecure-ports {
           rule-list block_bad_mgmt
       }
       reject-internal-net {
           action reject
           source {
               addresses {
                   172.27.0.0/16 { }
```

```
                }
            }
        }
    }
}
```

Displays the current list of management-firewall rules.

modify management-ip-rules rules delete { reject-internal-net }

Removes the reject-internal-net rule from the management-IP firewall.

Options

- **description**
  Your description for the management-firewall rules.
- **rules**
  Adds, deletes, or replaces a firewall rule.
  - **add**
    Creates a new rule, which you specify next with a unique string in curly braces ({}). Use the **place-before** or **place-after** option inside the curly braces to determine the order of the rule. If this is the first rule, use the **replace-all-with** option instead of **add**.
  - **delete**
    Deletes the rule that you specify next, in curly braces ({}).
  - **modify**
    Modifies the existing rule that you specify next, in curly braces ({}). After the rule name, enter the new configuration settings for the rule inside a nested set of curly braces.
  - **replace-all-with**
    Replaces the current set of global rules with the rule(s) that you specify next, in curly braces ({}). Use this option for the first management rule.
  - **none**
    Empties the list of management-firewall rules. This implicitly accepts all packets on the management interface.

  Enter the name of a rule to be added or modified, then enter an open curly brace ({), one or more of the following options, and a closed curly brace (}).
  - **action**
    Specifies the action that the system takes when a packet matches the rule.
    - **accept**
      Specifies that a matching packet should be accepted. The security software stops comparing a matching packet to any other management-firewall rules.
    - **accept-decisively**
      This option is functionally the same as **accept**.

- **drop**
  Specifies that a matching packet should be silently dropped. The security software sends nothing back to the packet source, and it does not compare the packet to any other managment-firewall rules.
- **reject**
  Specifies that a matching packet should be dropped. For TCP-based protocols, the security software sends a TCP reset (with the RST flag raised) back to the source. For other protocols, **reject** is equivalent to **drop**.

- **app-service**
  Associates the managment-rule list with a particular Application Service. An *Application Service* is a major component of an iApp, an advanced configuration tool for creating and maintaining similar applications on multiple servers. The *asm* module has components for working with iApps.
- **description**
  Your description for the current rule.
- **destination**
  Matches against each packet's destination IP and/or destination port. The next options choose the matching criteria.
  - **address-lists**
    Specifies a list of IP-address lists (see *address-list*) to compare against the packet's destination address.
    This list uses the same **add**, **delete**, **none**, and **replace-all-with** options described above for rules, as well as a **default** option.
  - **addresses**
    Specifies a list of IP addresses and/or subnets to compare against the packet's destination address.
    The format for an IPv4 address is *a*. *b*. *c*. *d* [/ *prefix*]. The general format for an IPv6 address is *a*: *b*: *c*: *d*: *e*: *f*: *g*: *h* [/ *prefix*]; you can shorten this by eliminating leading zeros from each field (for example, you can shorten "2001:0db7:3f4a:09dd:ca90:ff00:0042:8329" to "2001:db7:3f4a:9dd:ca90:ff00:42:8329"), and/or by removing the longest contiguous field of zeros (for example, you can shorten "2001:0:0:0:c34a:0:23ff:678" to "2001::c34a:0:23ff:678"). TMSH accepts any valid text representation of IPv6 addresses, as defined in RFC 2373 (see http://www.ietf.org/rfc/rfc2373.txt).
    To edit this list, use the same **add**, **delete**, **modify**, **none**, and **replace-all-with** options described above for rules.
  - **port-lists**
    Specifies a collection of port lists (see *port-list*) to compare against the packet's destination port. If you use this option to specify a port list, a packet only matches if it's destination port matches a port on these lists.
    This list uses the same **add**, **delete**, **none**, and **replace-all-with** options described above for rules, as well as a **default** option.

- **ports**
  Specifies a list of ports and port ranges to compare against the packet's destination port.
  To edit this list, use the same **add**, **delete**, **modify**, **none**, and **replace-all-with** options described above for rules.

- **icmp**
  Specifies a list of ICMP types and codes to compare against the packet. You must set the **ip-protocol** option to "icmp" for this option to function. If you use this option, the current rule only matches ICMP packets that have the ICMP properties you specify here. You can **add**, **delete**, or **modify** (that is, change the description of) any entry in the list, or **replace-all-with** a new set of entries that you specify between curly braces ({}).
  Use the standard integer identifiers to specify an ICMP type. For example: 3 is destination unreachable and 3:1 is destination unreachable with a code of host unreachable. The official list of ICMP types and codes is here: http://www.iana.org/assignments/icmp-parameters/icmp-parameters.xml.

- **ip-protocol**
  Specifies the IP protocol to compare against the packet. This could be a layer-3 protocol (such as ipv4 or ipv6), or a higher-level protocol like ospf, rdp, or icmp. If you specify this option, a packet only matches if it uses the chosen protocol. Press the <tab> key for a full list of valid protocols.

- **log**
  Specifies whether the security software should write a log entry for all packets that match this rule. You must also enable **network filter** logging in the *profile* component for this option to have any effect. Note that the security software always increments the statistics counter when a packet matches a rule, no matter how you set this option.

- **place-after [first | last | rule-name]**
  Specifies that a new rule should be placed after the **first** rule, the **last** rule, or the *rule-name* you specify. If you are adding individual rules (as opposed to specifying **replace-all-with**), then you must use **place-before** or **place-after** to specify the rule's position in the list.

- **place-before [first | last | rule-name]**
  Specifies that a new rule should be placed before the **first** rule, the **last** rule, or the *rule-name* you specify. If you are adding individual rules (as opposed to specifying **replace-all-with**), then you must use **place-before** or **place-after** to specify the rule's position in the list.

- **rule-list**
  Specifies a full rule list instead of a customized rule that you might define with the other options. See *rule-list*. If you use this option, then only the **schedule** and **status** options are valid; the tmsh software rejects any other options that you attempt to use with **rule-list**.

- **schedule**
  Specifies a schedule for the rule. See *schedule*. If you omit this option, the rule or rule list is enabled all the time.
  If the rule refers to a **rule-list**, the **rule-list** is enabled according to the schedule. When the **rule list** is enabled, the security software then honors the schedules defined within the **rule-list**.
- **source**
  Matches against each packet's source IP, source port, and/or source VLAN. The next options choose the matching criteria.
  - **address-lists**
    Specifies a list of address lists (see *address-list*) to compare against the packet's source address.
    This list uses the same **add**, **delete**, **none**, and **replace-all-with** options described above for rules, as well as a **default** option.
  - **addresses**
    Specifies a list of IP addresses and networks to compare against the packet's source address.
    The format for an IPv4 address is *a*. *b*. *c*. *d*. The general format for an IPv6 address is *a*: *b*: *c*: *d*: *e*: *f*: *g*: *h*.
    To edit this list, use the same **add**, **delete**, **modify**, **none**, and **replace-all-with** options described above for rules.
  - **port-lists**
    Specifies a collection of port lists (see *port-list*) to compare against the packet's source port. If you use this option to specify a port list, a packet only matches if its source port matches a port on these lists.
    This list uses the same **add**, **delete**, **none**, and **replace-all-with** options described above for rules, as well as a **default** option.
  - **ports**
    Specifies a list of ports and port ranges to compare against the packet's source port.
    To edit this list, use the same **add**, **delete**, **modify**, **none**, and **replace-all-with** options described above for rules.
  - **vlans**
    Specifies a list of VLANs, VLAN groups, and tunnels to compare against the packet.
    This list uses the same **add**, **delete**, **none**, and **replace-all-with** options described above for rules, as well as a **default** option.
- **status**
  Specifies whether the rule is **enabled**, **disabled** or **scheduled**. A rule that is **enabled** is always checked. A rule that is **disabled** is never checked. A rule that is **scheduled** is checked according to the corresponding schedule configuration. A rule that is **scheduled** must have an associated schedule configuration.

See Also

config-sync, *device-group*, *edit*, *list*, *modify*, *address-list*, *port-list*, *rule-list*, *profile*, *schedule*, *tmsh*

matching-rule

Shows the best match firewall rule amongst all the admin configured Network Firewall rules in different contexts (global, route-domain, VIP/SelfIP) given source/destination IP address and port, protocol and user configured vlan name. You can only use the **show** command with this component.

Syntax

```
show matching-rule
     dest-addr [IP address]
     source-addr [IP address]
     dest-port [TCP/UDP port]
     source-port [TCP/UDP port]
     protocol [protocol]
     vlan [vlan name]
```

Description

With user provided VLAN, source/destination IP addresses, TCP/UDP ports and protocol, the command will try to match these parameters against user configured ACL rules in global, route domain, VIP/SelfIP context, and return the best match rules. Both IPv4 and IPv6 addresses and all possible protocols are supported. This command can be used as a diagnostic tool to trouble-shoot BigIP firewall configuration problem. It provides a faster way to identify which ACL rule will have impact to the specified packet stream.

Examples

show security firewall matching-rule dest-addr 1.1.1.1 dest-port 140 source-addr 2.2.2.2 source-port 141 protocol 10 vlan /Common/internal

```
Firewall Matching Rule:
-------------------------------------------------------
Context Type  Context Name  Policy Name  Rule Name   Action
-------------------------------------------------------
Global                                   globalrule  Accept
Total records returned: 1
```

See Also

show, *tmsh*

policy

Configures firewall policy.

Syntax

Modify the policy component within the **security firewall** module using the syntax shown in the following sections.

Create/Modify

```
create policy [name]
  copy-from [string]
modify policy [name]
  description [string]
  rules [add | delete | modify | replace-all-with] {
     [ [name] ] {
        action [accept | accept-decisively | drop | reject]
        description [string]
        destination {
          address-lists [add | default | delete | replace-all-with] {
            [address list names...]
          }
          address-lists none
          addresses [add | default | delete | replace-all-with] {
            [ [ip address] | [ip address/prefixlen] ]
          }
          addresses none
          geo [add | default | delete | replace-all-with] {
            [ [country_code [state state_name] ] ]
          }
          geo none
          port-lists [add | default | delete | replace-all-with] {
            [port list names...]
          }
          port-lists none
          ports [add | default | delete | none | replace-all-with] {
            [ [port] | [port1-port2] ]
          }
          ports none
        }
        icmp [add | delete | modify | replace-all-with] {
          [ [icmp_type] | icmp_type:icmp_code ] {
            description [string]
          }
        }
        icmp none
        ip-protocol [protocol name]
        irule [irule name]
        irule-sample-rate [integer]
        log [no | yes]
        place-after [first | last | [rule name]]
        place-before [first | last | [rule name]]
        rule-list [rule list name]
        schedule [schedule name]
        source {
          address-lists [add | default | delete | replace-all-with] {
```

```
            [address list names...]
          }
          address-lists none
          addresses [add | default | delete | replace-all-with] {
            [ [ip address] | [ip_address/prefixlen] ]
          }
          addresses none
          geo [add | default | delete | replace-all-with] {
            [ [country_code [state state_name] ] ]
          }
          geo none
          port-lists [add | default | delete | replace-all-with] {
            [port list names...]
          }
          port-lists none
          ports [add | default | delete | replace-all-with] {
            [ [port] | [port1-port2] ]
          }
          ports none
          vlans [add | default | delete | replace-all-with] {
            [vlan names...]
          }
          vlans none
        }
        status [disabled | enabled | scheduled]
      }
    }
    rules none
  edit policy
      all-properties
      non-default-properties
```

Display

```
list policy
show running-config policy
  all-properties
  non-default-properties
  one-line
```

Description

You can use the **policy** component to configure a sharable and reusable set of network firewall rules which can be associated as enforced or staged with a number of configuration objects of the following types: **net self**, **ltm virtual**, **security firewall global-rules**, **net route-domain**.

Examples

```
modify policy rules add {
 reject-internal-net {
   place-before first
   action reject
   source {
```

```
    addresses replace-all-with { 172.27.0.0/16 }
  }
}
```

Creates a rule entry at the beginning of the list that rejects traffic from the 172.27.0.0 network.

modify policy rules delete reject-internal-net

Removes the rule reject-internal-net from the list of rules.

create security firewall policy p1 rules add { r1 { source { geo add { US } } action reject place-after first } }Creates a policy with a single rule that rejects all packets from the US.

list policy

Displays the current list of policy rules.

create policy "New Policy" copy-from "/Common/Existing Policy"

Creates a new policy **New Policy** by copying existing policy **/Common/Existing Policy**.

Options

- **description**
  User defined description.
- **copy-from**
  (**CREATE**)Specifies the name of an existing policy from which to copy all configuration options.
- **rules**
  Adds, deletes, or replaces a firewall rule.
  - **action**
    Specifies the action that the system takes when a rule is matched.
    - **accept**
      Specifies that the current packet should be accepted.
    - **accept-decisively**
      Specifies that the current packet should be accepted and that packet will not be compared to any other firewall rules in any other context.
    - **drop**
      Specifies that the current packet should be silently dropped. Nothing is sent back to the packet source. The packet is not compared to any other firewall rules.
    - **reject**
      Specifies that the current packet should be dropped. For TCP based protocols a TCP reset is sent to the source. For other protocols **reject** is equivalent to **drop**.
  - **description**
    User defined description.

- **destination**

  - **address-lists**
    Specifies a list of address lists (see **security firewall address-list**) against which the packet will be compared.
  - **addresses**
    Specifies a list of addresses and networks against which the packet will be compared.
  - **geo**
    Specifies a list of Geo Locations that the packet will be compared against."
  - **port-lists**
    Specifies a list of port lists (see **security firewall port-list**) against which the packet will be compared.
  - **ports**
    Specifies a list of ports and port ranges against which the packet will be compared.

- **icmp**
  Specifies a list of ICMP types and codes against which the packet will be compared. The standard integer identifiers are used to specify an ICMP type Example: 3 is destination unreachable and 3:1 is destination unreachable with a code of host unreachable. The list of ICMP types and codes can be found here http://www.iana.org/assignments/icmp-parameters/icmp-parameters.xml.
- **ip-protocol**
  Specifies the IP protocol against which the packet will be compared.
- **irule**
  Specifies the name of the iRule that will be triggered when a packet matches this firewall rule. The firewall rule match raises a FLOW_INIT iRule event.
- **irule-sample-rate**
  Specifies the rate at which an iRule specified by **irule** option will be triggered when a packet matches this firewall rule. The rate is an integer value in the range 0-65535 and specifies how many packets must match this firewall rule before the iRule is triggered. The default value is 1 and causes the iRule to be triggered for every packet that matches this firewall rule. A value of 0 disables iRule triggering.
- **log**
  Specifies whether the packet will be logged if it matches the rule. Logging must also be enabled in the corresponding logging configuration. (e.g. **security log profile global-network** when policy assigned to **global-rules**). Note that the statistics counter is always incremented when a packet matches a rule.
- **place-after**
  Specifies that a new rule should be placed after another rule, **first** or **last**. If individual rules are being added (as opposed to specifying **replace-all-with**) then **place-before** or **place-after** must be specified.

- **place-before**
  Specifies that a new rule should be placed before another rule, **first** or **last**. If individual rules are being added (as opposed to specifying **replace-all-with**) then **place-before** or **place-after** must be specified.
- **rule-list**
  Specifies a list of rules to evaluate. See **security firewall rule-list**. If a **rule-list** is specified then only the **schedule** and **status** properties effect the rule.
- **schedule**
  Specifies a schedule for the rule. See **security firewall schedule**. If the rule refers to a **rule-list** the **rule-list** will be enabled according to the schedule. When the **rule list** is enabled, the schedules defined within the **rule-list** will be honored.
- **source**
  - **address-lists**
    Specifies a list of address lists (see **security firewall address-list**) against which the packet will be compared.
  - **addresses**
    Specifies a list of addresses and networks against which the packet will be compared.
  - **geo**
    Specifies a list of Geo Locations against which the packet will be compared.
  - **port-lists**
    Specifies a list of port lists (see **security firewall port-list**) against which the packet will be compared.
  - **ports**
    Specifies a list of ports and port ranges against which the packet will be compared.
  - **vlans**
    Specifies a list of vlans, vlan groups and tunnels against which the packet will be compared.
- **status**
  Specifies whether the rule is **enabled**, **disabled** or **scheduled**. A rule that is **enabled** is always checked. A rule that is **disabled** is never checked. A rule that is **scheduled** is checked according to the corresponding schedule configuration. A rule that is **scheduled** must have an associated schedule configuration.

See Also

create, *edit*, *list*, *modify*, *address-list*, *port-list*, *rule-list*, *profile*, *schedule*, *tmsh*

port-list

Configures a port-list for use by firewall rules. A firewall rule can match a packet's source port or destination port against one of the ports in a port list, and can take some action (such as ACCEPT or DROP) for a matching packet.

Syntax

Create/Modify

```
create port-list [name]
modify port-list [[name] | all]
  app-service [name]
  description [string]
  ports [add | delete | modify | replace-all-with] {
   [ [port] | [port] - [port] ]
  }
edit port-list [[name] | all]
    all-properties
    non-default-properties
```

Display

```
list port-list [[name] | all | [property]]
show running-config port-list [[name] | all | [property]]
```

Delete

```
delete port-list [[name] | all]
```

Description

You can use the **port-list** component to define reusable lists of ports for various firewall rules. The network software compares a packet's source port and/or destination port against ports in this list. You can assign a port list to the firewall rules in **net self**, **net route-domain**, **security firewall global-rules**, **security firewall rule-list**, **sys management-ip**, and **ltm virtual** firewall rules.

Examples

create port-list p-list1 ports add { 80 }

Creates a new port list with one entry.

```
list port-list
security firewall port-list _sys_self_allow_tcp_defaults {
   ports {
        domain { }
```

```
        f5-iquery { }
        https { }
        snmp { }
        ssh { }
    }
}
security firewall port-list _sys_self_allow_udp_defaults {
    ports {
        520 { }
        cap { }
        domain { }
        f5-iquery { }
        snmp { }
    }
}
security firewall port-list p-list1 {
    ports {
        http { }
    }
}
```

Shows all the port lists, including the one created in the previous example.

Options

- **app-service**
  Associates this port list with a particular Application Service. An *Application Service* is a major component of an iApp, an advanced configuration tool for creating and maintaining similar applications on multiple servers. The *asm* module has components for working with iApps.
- **description**
  Your description for the port list.
- **ports**
  Specifies a list of ports to compare against a packet's source or destination port. Use one of the keywords below and then specify the port(s) to add or delete. Specify ranges of ports with a dash between the two ends of the range (for example, 80-88).
  - **add**
    Creates a new port list, which you specify next with port numbers in curly braces ({}).
  - **delete**
    Deletes the port(s) that you specify next, in curly braces ({}).
  - **modify**
    Is not supported for this component.
  - **replace-all-with**
    Replaces the current set of ports with the port(s) that you specify next, in curly braces ({}).

See Also

edit, *list*, *modify*, *self*, *route-domain*, *address-list*, *rule-list*, *global-rules*, *tmsh*

rule-list

Configures a rule-list of network firewall rules. You can reuse a rule list in multiple firewalls, such as the firewalls for self IPs, routing domains, and the global firewall.

Syntax

Create/Modify

```
create rule-list [name]
modify rule-list [[name] | all]
  description [string]
  rules [add | delete | modify | replace-all-with] {
     [ [name] ] {
        action [accept | accept-decisively | drop | reject]
        app-service [name]
        description [string]
        source {
          address-lists [add | default | delete | replace-all-with] {
            [address list names...]
          }
          address-lists none
          addresses [add | delete | modify | replace-all-with] {
            [ [ip address] | [ip_address/prefixlen] ]
          }
          addresses none
          geo [add | default | delete | replace-all-with] {
            [ [country_code [state state_name] ] ]
          }
          geo none
          port-lists [add | default | delete | replace-all-with] {
            [port list names...]
          }
          port-lists none
          ports [add | default | delete | replace-all-with] {
            [ [port] | [port1-port2] ]
          }
          ports none
          vlans [add | default | delete | replace-all-with] {
            [vlan names...]
          }
          vlans none
        }
        destination {
          address-lists [add | default | delete | replace-all-with] {
            [address list names...]
          }
          address-lists none
          addresses [add | delete | modify | replace-all-with] {
            [ [ip address] | [ip address/prefixlen] ]
          }
          addresses none
          geo [add | default | delete | replace-all-with] {
            [ [country_code [state state_name] ] ]
          }
          geo none
```

```
            port-lists [add | default | delete | replace-all-with] {
              [port list names...]
            }
            port-lists none
            ports [add | delete | modify | replace-all-with] {
              [ [port] | [port1-port2] ]
            }
            ports none
          }
          icmp [add | delete | modify | replace-all-with] {
            [ [icmp_type] | icmp_type:icmp_code ] {
              description [string]
            }
          }
          icmp none
          ip-protocol [protocol name]
          irule [irule name]
          irule-sample-rate [integer]
          log [no | yes]
          place-after [first | last | [rule name]]
          place-before [first | last | [rule name]]
          rule-list [rule list name]
          schedule [schedule name]
          status [disabled | enabled | scheduled]
      }
    }
    rules none
edit rule-list [[name] | all]
    all-properties
    non-default-properties
```

Display

```
list rule-list [[name] | all | [property]]
show running-config rule-list [[name] | all | [property]]
```

Description

You can use the **rule-list** component to configure network firewall rules to be applied to multiple firewalls. The network software compares IP packets to the criteria specified in these rules. If a packet matches the criteria then the system takes the action specified by the rule. If a packet does not match any rule in the list, the software accepts the packet or passes it to the next rule or rule-list (for example, the system compares the packet to **net self-ip** rules if the packet is destined for a network associated with a **self-ip** that has firewall rules defined).

Matching An Ip Packet

You can use this TMSH component to match against any or all of the following properties of an IP packet:

- source address

- source geo
- source port
- the packet's source VLAN
- destination address
- destination geo
- destination port
- the higher-level protocol in the packet's payload

If you match against more than one of these items, a packet must pass *all* of your tests to successfully match. For example, if you match against a source subnet and several destination ports, a packet must originate from the given subnet and must also have one of the specified destination ports.

Rule Order

The network software evaluates firewall rules in the order that you specify. You can use the **list management-ip-rules** command to see the current rule order. As you add or modify rules in this component, you can use the **place-before** *rule-name* or **place-after** *rule-name* option to choose the rule's place in the sequence.

Rule order can determine whether or not a packet is dropped. Consider the following rules:

- rule_a, matches source addresses against 172.16.0.0 and ACCEPTS all packets that match.
- rule_d, matches source addresses against 172.16.39.0 and DROPS all packets that match.

Also consider a packet from a host at 172.16.39.55. If rule_a appears before rule_d in the rule list, the packet's source address matches rule_a first and the software accepts it. The software never reaches rule_d for comparison. If rule_d appears first instead, the packet's source address now matches rule_d; in this case, the software drops the packet.

Examples

create rule-list block_bad_mgmt description "ports to be blocked on our management interfaces" rules replace-all-with { reject_telnet { ip-protocol tcp destination { ports add { telnet } } action reject } }

Creates a new rule list called block_bad_mgmt. It matches and rejects any TCP packet whose destination port is telnet. The description indicates that the rule is intended for the management-IP firewall.

modify rule-list block_bad_mgmt rules add { reject_http { ip-protocol tcp destination { ports add { http } } action reject place-after last } }

Modifies the above rule list by blocking HTTP traffic, too.

```
list rule-list block_bad_mgmt
security firewall rule-list block_bad_mgmt {
   description "ports to be blocked on our management interfaces"
   rules {
       reject_telnet {
           action reject
           destination {
               ports {
                   telnet { }
               }
           }
           ip-protocol tcp
       }
       reject_http {
           action reject
           destination {
               ports {
                   http { }
               }
           }
           ip-protocol tcp
       }
   }
}
```

Shows the above rule list, with both rules.

modify rule-list rules add { reject-internal-net { place-before first action reject source { addresses replace-all-with { 172.27.0.0/16 } } } }

Creates a rule entry at the beginning of the list that rejects traffic from the 172.27.0.0 network.

create security firewall rule-list rl1 description "Geo Locations to be blocked" rules add { r1 { source { geo add { US } } place-after first action drop } }

Creates a new rule list "rl1", which matches and rejects any packet with a US source. The description explains the purpose of the rule list.

modify security firewall rule-list rl2 rules add { r2 { source { geo add { CA } } place-before last action drop } }

```
security firewall rule-list rl2 {
description "Geo Locations to be blocked"
   rules {
       r2 {
           action drop
           source {
               geo {
                   CA {
                       state none
                   }
               }
           }
```

```
        }
        r1 {
            action drop
            source {
                geo {
                    US {
                        state none
                    }
                }
            }
        }
    }
}
```

Shows the above rule list, with both rules.

Options

- **app-service**
  Associates the rule list with a particular Application Service. An *Application Service* is a major component of an iApp, an advanced configuration tool for creating and maintaining similar applications on multiple servers. The *asm* module has components for working with iApps.
- **description**
  Your description for this list of firewall rules.
- **rules**
  Adds, deletes, or replaces a firewall rule.
  - **add**
    Creates a new rule, which you specify next with a unique string in curly braces ({}). Use the **place-before** or **place-after** option inside the curly braces to determine the order of the rule. If this is the first rule, use the **replace-all-with** option instead of **add**.
  - **delete**
    Deletes the rule that you specify next, in curly braces ({}).
  - **modify**
    Modifies the existing rule that you specify next, in curly braces ({}). After the rule name, enter the new configuration settings for the rule inside a nested set of curly braces.
  - **none**
    Empties the list of rules. An empty rule list implicitly accepts all packets. The security software skips this context and assesses packets against the next layer of firewall rules, if there is one (such as those defined for **net self-ip**, **net route-domain** or **ltm virtual**)
  - **replace-all-with**
    Replaces the current list of rules with the rule(s) that you specify next, in curly braces ({}). Use this option for the first rule in the list.

Enter the name of a rule to be added or modified, then enter an open curly brace ({), one or more of the following options, and a closed curly brace (}).

- **action**
  Specifies the action that the system takes when a rule is matched.
  - **accept**
    Specifies that a matching packet should be accepted. The security software stops comparing a matching packet to any other rules in the list. The software continues comparing the packet to rules in the next appropriate context (such as **net self-ip**, **net route-domain** or **ltm virtual**).
  - **accept-decisively**
    Specifies that a matching packet should be accepted and should not be compared to any other firewall rules in any other context.
  - **drop**
    Specifies that a matching packet should be silently dropped. The security software sends nothing back to the packet source. The security software does not compare the packet to any other firewall rules in any other context.
  - **reject**
    Specifies that a matching packet should be dropped. For TCP-based protocols, the security software sends a TCP reset (with the RST flag raised) back to the source. For other protocols, **reject** is equivalent to **drop**.
- **description**
  Your description for the current rule.
- **destination**
  Matches against each packet's destination IP and/or destination port. The next options choose the matching criteria.
  - **address-lists**
    Specifies a list of IP-address lists (see *address-list*) to compare against the packet's destination address.
    This list uses the same **add**, **delete**, **none**, and **replace-all-with** commands described above for rules, as well as a **default** command.
  - **addresses**
    Specifies a list of IP addresses and/or subnets to compare against the packet's destination address.
    The format for an IPv4 address is *a*. *b*. *c*. *d* [/ *prefix*]. The general format for an IPv6 address is *a*: *b*: *c*: *d*: *e*: *f*: *g*: *h* [/ *prefix*]; you can shorten this by eliminating leading zeros from each field (for example, you can shorten "2001:0db7:3f4a:09dd:0a90:ff00:0042:8329" to "2001:db7:3f4a:9dd:a90:ff00:42:8329"), and/or by removing the longest contiguous field of zeros (for example, you can shorten "2001:0:0:0:c34a:0:0:678" to "2001::c34a:0:0:678"). TMSH accepts any valid text representation of IPv6 addresses, as defined in RFC 2373 (see http://www.ietf.org/rfc/rfc2373.txt).
    To edit this list, use the same **add**, **delete**, **modify**, **none**, and **replace-all-with** commands described above for rules.

- **geo**
  Specifies a list of Geo Locations to compare a packet's source or destination Geo Location.
  The format for a Geo Location is a 2 character string for the country code and a string for the state.
  To edit this list, use the same **add**, **delete**, **modify**, **none**, and **replace-all-with** options described above for rules.
- **port-lists**
  Specifies a collection of port lists (see *port-list*) to compare against the packet's destination port. If you use this option to specify a port list, a packet only matches if it's destination port matches a port on these lists.
  If you combine address lists and port lists in the same rule, a packet must have a matching port **and** a matching address to fully match the rule.
  This list uses the same **add**, **delete**, **none**, and **replace-all-with** commands described above for rules, as well as a **default** command.
- **ports**
  Specifies a list of ports and port ranges to compare against the packet's destination port.
  To edit this list, use the same **add**, **delete**, **modify**, **none**, and **replace-all-with** commands described above for rules.

- **icmp**
  Specifies a list of ICMP types and codes to compare against the packet. You must set the **ip-protocol** option to "icmp" for this option to function. If you use this option, the current rule only matches ICMP packets that have the ICMP properties you specify here. You can **add**, **delete**, or **modify** (that is, change the description of) any entry in the list, or **replace-all-with** a new set of entries that you specify between curly braces ({}).
  Use the standard integer identifiers to specify an ICMP type. For example: 3 is destination unreachable and 3:1 is destination unreachable with a code of host unreachable. The official list of ICMP types and codes is here:
  http://www.iana.org/assignments/icmp-parameters/icmp-parameters.xml.
- **ip-protocol**
  Specifies the IP protocol to compare against the packet. This could be a layer-3 protocol (such as ipv4 or ipv6), or a higher-level protocol like ospf or rdp. If you specify this option, a packet only matches if it uses the chosen protocol. Press the <tab> key for a full list of valid protocols.
- **irule**
  Specifies the name of the iRule that will be triggered when a packet matches this firewall rule. The firewall rule match raises a FLOW_INIT iRule event.

- **irule-sample-rate**
  Specifies the rate at which an iRule specified by **irule** option will be triggered when a packet matches this firewall rule. The rate is an integer value in the range 0-65535 and specifies how many packets must match this firewall rule before the iRule is triggered. The default value is 1 and causes the iRule to be triggered for every packet that matches this firewall rule. A value of 0 disables iRule triggering.
- **log**
  Specifies whether the security software should write a log entry for all packets that match this rule. You must also enable **network filter** logging in the *profile* component for this option to have any effect. Note that the security software always increments the statistics counter when a packet matches a rule, no matter how you set this option.
- **place-after [first | last | rule-name]**
  Specifies that a new rule should be placed after the **first** rule, the **last** rule, or the *rule-name* you specify. If you are adding individual rules (as opposed to specifying **replace-all-with**), then you must use **place-before** or **place-after** to specify the rule's position in the list.
- **place-before [first | last | rule-name]**
  Specifies that a new rule should be placed before the **first** rule, the **last** rule, or the *rule-name* you specify. If you are adding individual rules (as opposed to specifying **replace-all-with**), then you must use **place-before** or **place-after** to specify the rule's position in the list.
- **rule-list**
  Specifies a full rule list instead of a customized rule that you might define with the other options. If you use this option, then only the **schedule** and **status** options are valid; the tmsh software rejects any other options that you attempt to use with **rule-list**.
- **schedule**
  Specifies a schedule for the rule. See *schedule*. If you omit this option, the rule or rule list is enabled all the time.
  If the rule refers to a **rule-list**, the **rule-list** is enabled according to the schedule. When the **rule list** is enabled, the security software then honors any schedules defined within the **rule-list**.
- **source**
  Matches against each packet's source IP, source port, and/or source VLAN. The next options choose the matching criteria.
  - **address-lists**
    Specifies a list of address lists (see *address-list*) to compare against the packet's source address.
    This list uses the same **add**, **delete**, **none**, and **replace-all-with** commands described above for rules, as well as a **default** command.
  - **addresses**
    Specifies a list of IP addresses and networks to compare against the packet's source address.
    The format for an IPv4 address is *a*. *b*. *c*. *d*. The format for an IPv6

address is *a*: *b*: *c*: *d*: *e*: *f*: *g*: *h*.
To edit this list, use the same **add**, **delete**, **modify**, **none**, and **replace-all-with** commands described above for rules.

- **geo**
  Specifies a list of Geo Locations to compare a packet's source or destination Geo Location.
  The format for a Geo Location is a 2 alphabet string for the country code and a string for the state.
  To edit this list, use the same **add**, **delete**, **modify**, **none**, and **replace-all-with** options described above for rules.
- **port-lists**
  Specifies a collection of port lists (see *port-list*) to compare against the packet's source port. If you use this option to specify a port list, a packet only matches if its source port matches a port on these lists.
  This list uses the same **add**, **delete**, **none**, and **replace-all-with** commands described above for rules, as well as a **default** command.
- **ports**
  Specifies a list of ports and port ranges to compare against the packet's source port.
  To edit this list, use the same **add**, **delete**, **modify**, **none**, and **replace-all-with** commands described above for rules.
- **vlans**
  Specifies a list of VLANs, VLAN groups, and tunnels to compare against the packet.
  This list uses the same **add**, **delete**, **none**, and **replace-all-with** commands described above for rules, as well as a **default** command.

- **status**
  Specifies whether the rule is **enabled**, **disabled** or **scheduled**. A rule that is **enabled** is always checked. A rule that is **disabled** is never checked. A rule that is **scheduled** is checked according to the corresponding schedule configuration. A rule that is **scheduled** must have an associated schedule configuration.

See Also

edit, *list*, *modify*, *address-list*, *port-list*, *global-rules*, *profile*, *schedule*, *tmsh*

rule-stat

Displays statistics of firewall rules on the BIG-IP® system. You can only use the **show** command with this component.

Syntax

```
show rule-stat
    (default | exa | gig | kil | meg | peta | raw | tera | yotta | zetta)
    field-fmt
```

Description

You can use the **rule-stat** component to display statistics of firewall rules.

Examples

show rule-stat

Displays firewall rule's statistics in the system default units.

show rule-stat raw

Displays raw firewall rule's statistics.

See Also

show, *tmsh*

schedule

Create a schedule that you can apply to firewall rules.

Syntax

Create/Modify

```
create schedule [name]
modify schedule [[name] | all]
  app-service [name]
  daily-hour-end [hour:minute]
  daily-hour-start [hour:minute]
  date-valid-end [MM/DD/YYYY]
  date-valid-start [MM/DD/YYYY]
  description [text]
  days-of-week [ [monday | tuesday | wednesday | thursday | friday | saturday | sunday]
... ]
edit schedule [ [name] | [glob] | [regex] ] ... ]
```

Display

```
list schedule [[name] | all | [property]]
```

Delete

```
delete schedule [[name] | all]
show running-config schedule [[name] | all | [property]]
```

Description

You use the **schedule** component to specify when to apply a firewall rule. You can specify a start time and an end time, some days of the week, a date when the schedule first starts, and/or a date when the schedule ends forever.

To apply the schedule to a firewall rule or rule list, edit the firewall or rule-list component. These are the firewalls and rule lists where you can apply schedules:

- *global-rules*
- *management-ip-rules*
- *self*
- *route-domain*
- *virtual*

- *rule-list*

By default, all firewall rules are continuously active. By applying a schedule to a firewall rule, you reduce the time that the rule is running.

If you create a schedule without any scheduling specifications (such as **daily-hour-start**), the schedule is always active.

Note you may not delete a **schedule** that is being used by any firewall rule or rule list.

Examples

create schedule my_schedule1 date-valid-start now date-valid-end 12/31/2016 daily-hour-start 8:00 daily-hour-end 17:00

Creates a new schedule which is active between 8am and 5pm every day until December 31, 2016.

```
list schedule>
security firewall schedule my_schedule1 {
   daily-hour-end 17:00
   daily-hour-start 8:00
   date-valid-end 2016-12-31:00:00:00
   date-valid-start 2012-12-12:08:40:01
}
security firewall schedule workHours {
   daily-hour-end 18:00
   daily-hour-start 8:00
   days-of-week { monday tuesday wednesday thursday friday }
}
```

Lists two user-configured schedules, including the one that you created above.

modify schedule my_schedule1 days-of-week { monday tuesday wednesday }

Modifies the schedule named "my_schedule1." This limits the schedule to running only
on Mondays, Wednesdays, and Fridays.

Options

- **app-service**
  Associates this schedule with a particular Application Service. An *Application Service* is a major component of an iApp, an advanced configuration tool for creating and maintaining similar applications on multiple servers. The *asm* module has components for working with iApps.
- **description**
  Describes the schedule.
- **daily-hour-end**
  Specifies the time of day this schedule stops. This end hour must be after the **daily-hour-start** value. The default is 24:00 (midnight).

A schedule may not contain hours that go past midnight (24:00): for example, a daily-hour-start of 20:00 and daily-hour-end of 02:00 is not allowed. If you need to cover both the late hours and early hours of the day, please create two schedules.

- **daily-hour-start**
  Specifies the time of day this schedule starts. This start hour must be before the **daily-hour-end** value. The default is 0:00 (midnight at the start of the day).
- **date-valid-end**
  Specifies the final date for this schedule. The schedule stops firing as of this date. You may specify just the specific date, or a specific date and time for the schedule to end. The date must be after the **date-valid-start** value. The default is 19:14 1/18/2038 (the latest date expressible with a 32-bit integer).
- **date-valid-start**
  Specifies the start date for this schedule. The schedule does not fire before this date and time. You may specify just the specific date, or a specific date and time for the schedule to start. You must specify a date before the **date-valid-end value**. The default is midnight 1/1/1970 (Unix epoch).
- **days-of-week**
  Specifies which days of the week the schedule fires. You must specify at least one day of the week, and you cannot specify any day of the week more than once. The default is all seven days.

See Also

create, *delete*, *edit*, *list*, *modify*, *self*, *route-domain*, *global-rules*, *management-ip-rules*, *rule-list*, *virtual*, *tmsh*

user-domain

Configures a user-domain for use by firewall rules.

Syntax

Create/Modify

```
create user-domain [name]
modify user-domain [[name] | all]
  domain string
  ifmap-service [add | delete | modify | replace-all-with] {
          [ip]
          [port]
          [login]
          [password]
  }
  app-service [name]
  description [string]
edit user-domain [[name] | all]
    all-properties
    non-default-properties
```

Display

```
list user-domain [[name] | all | [property]]
show running-config user-domain [[name] | all | [property]]
```

Delete

```
delete user-domain [[name] | all]
```

Run

```
run user-domain [[name] | all] clear-cache
```

Description

A *user-domain* object holds attributes to reach services that provide more information about a user. This information includes the domain for which the service is defined, the identity service that can be used to validate this user and the ifmap service that can be used to obtain more information about the user. User domains also have associated cache data which is utilized by user identity feature for performance improvements. You can use the **user-domain** component to define reusable configuration that is used to learn about more users used in the firewall rules or clear their associated cache data on demand.

Examples

create user-domain gladiators identity-server add { felix-legions { ip 1.1.1.1 login maximus password meridius port 10002 } }

Creates a new user-domain object that defines a new identity-server for domain *gladiators* with an identity service *felix-legions*

modify user-domain gladiators ifmap-server add { rome { ip 10.10.10.10 login marcus password aurelius port 10002 } }

Modifies the above user domain to add an ifmap server.

run user-domain grumpycat clear-cache

Clears the user identity cache associated with a specified user domain name.

run user-domain all clear-cache

Clears the user identity cache for all available user domains.

Options

- **domain**
  Specifies a domain for which the identity and ifmap services are defined.
- **app-service**
  Associates this user domain with a particular Application Service. An *Application Service* is a major component of an iApp, an advanced configuration tool for creating and maintaining similar applications on multiple servers. The **asm** module (see *asm*) has components for working with iApps.
- **description**
  User-defined description for this user domain.
- **clear-cache**
  Invokes clear-cache functionality for the given user-domain name.

See Also

edit, *list*, *modify*, *self*, *route-domain*, *global-rules*, *management-ip-rules*, *rule-list*, *virtual*, *tmsh*

user-list

Configures a user-list for use by firewall rules. A firewall rule can match a packet sourced from a particular user against one of the users or user-groups in a user list, and can take some action (such as ACCEPT or DROP) for a matching packet. An incoming packet's souce IP address is matched in user identity database to get the user and group properties which are then used to perform the rule match.

Syntax

Create/Modify

Display

```
list user-list [[name] | all | [property]]
```

Delete

```
delete user-list [[name] | all]
```

Description

You can use the **user-list** component to define reusable lists of user or user-group names for various firewall rules. The network software compares a packet's source user (mapped by incoming source IP address) and group that user belong to, against users (or user-groups) in this list. You can assign a user list to the firewall rules in **net self**, **net route-domain**, **security firewall global-rules**, **security firewall rule-list**, and **ltm virtual** firewall rules.

Examples

create user-list u-list1 users add { olympus}

Creates a new user list named **u-list1** with one user named **xyz** in domain **olympus**.

create user-list u-list2 user-groups add { olympuseng }

Creates a new user list named **u-list2** with one group named **eng** in domain **olympus**.

list user-list

Shows all the user lists configured in the system.

Options

- **app-service**
  Associates this user list with a particular Application Service. An *Application Service* is a major component of an iApp, an advanced configuration tool for creating and maintaining similar applications on multiple servers. The *asm* module has components for working with iApps.
- **description**
  Your description for the user list.
- **user-groups**
  Specifies a list of user groups to compare against the groups a user belongs to (which is mapped from the source IP address).
- **users**
  Specifies a list of users to compare against a packet's source user (which is mapped from the source IP address).

See Also

edit, *list*, *modify*, *self*, *route-domain*, *address-list*, *rule-list*, *global-rules*, *tmsh*

86

security http

- Introducing the security http module
- Alphabetical list of components

Introducing the security http module

You can use the tmsh components that reside within the security http module to configure the Security HTTP feature.

For more information about the tmsh hierarchical structure, see Chapter 2, *Understanding and Using the Traffic Management Shell*.

Alphabetical list of components

The remainder of this chapter lists the tmsh components that are available in the security http module.

file-type

Lists the available file types that can be used in the context of HTTP Protocol Security.

Syntax

Retrieve the list of the **file-type** values using the syntax shown in the following sections.

Display

```
list file-type
list file-type [ [ [name] | [glob] | [regex] ] ... ]
    all
    app-service
    one-line
```

Description

Use this command to display the possible values of the file-type object to be used in the context of HTTP Protocol Security. These possible values include predefined and user-defined file types that you can select to have the security profiles allow or disallow.

Examples

list file-type

Displays all the file types supported by HTTP Protocol Security.

Options

- **app-service**
  Displays the application service to which the object belongs. The default value is **none**. **Note:** If the **strict-updates** option is **enabled** on the Application Service that owns the object, you cannot modify or delete the object. Only the Application Service can modify or delete the object.

See Also

glob, *list*, regex, *profile*, *tmsh*

mandatory-header

Lists the available mandatory headers that can be used in the context of HTTP Protocol Security.

Syntax

Retrieve the list of the **mandatory-header** values using the syntax shown in the following sections.

Display

```
list mandatory-header
list mandatory-header [ [ [name] | [glob] | [regex] ] ... ]
    all
    app-service
    one-line
```

Description

Use this command to display the possible values of the mandatory-header object to be used in the context of HTTP Protocol Security. These possible values include predefined and user-defined HTTP headers that you can select to be required by the security profiles.

Examples

list mandatory-header

Displays all the mandatory headers supported by HTTP Protocol Security.

Options

- **app-service**
  Displays the application service to which the object belongs. The default value is **none**. **Note:** If the **strict-updates** option is **enabled** on the Application Service that owns the object, you cannot modify or delete the object. Only the Application Service can modify or delete the object.

See Also

glob, *list*, regex, *profile*, *tmsh*

profile

Configures an HTTP security profile.

Syntax

Configure the **profile** component within the **security http** module using the syntax shown in the following sections.

Create/Modify

```
create profile [name]
modify profile [name]
    app-service [[string] | none]
    [case-sensitive | case-insensitive]
    defaults-from [[name] | none]
    description [[string] | none]
    evasion-techniques {
        alarm [disabled | enabled]
        block [disabled | enabled]
    }
    file-types {
        alarm [disabled | enabled]
        [allowed | disallowed]
        block [disabled | enabled]
        values [add | delete | none | replace-all-with] { [string] ... }
    }
    http-rfc {
        alarm [disabled | enabled]
        bad-host-header [disabled | enabled]
        bad-version [disabled | enabled]
        block [disabled | enabled]
        body-in-get-head [disabled | enabled]
        chunked-with-content-length [disabled | enabled]
        content-length-is-positive [disabled | enabled]
        header-name-without-value [disabled | enabled]
        high-ascii-in-headers [disabled | enabled]
        host-header-is-ip [disabled | enabled]
        maximum-headers [[integer] | disabled]
        null-in-body [disabled | enabled]
        null-in-headers [disabled | enabled]
        post-with-zero-length [disabled | enabled]
        several-content-length [disabled | enabled]
        unparsable-content [disabled | enabled]
    }
    mandatory-headers {
        alarm [disabled | enabled]
        block [disabled | enabled]
        values [add | delete | none | replace-all-with] { [string] ... }
    }
    maximum-length {
        alarm [disabled | enabled]
        block [disabled | enabled]
        post-data [[integer] | any]
        query-string [[integer] | any]
        request [[integer] | any]
        uri [[integer] | any]
```

```
    }
    methods {
        alarm [disabled | enabled]
        block [disabled | enabled]
        values [add | delete | none | replace-all-with] { [string] ... }
    }
    response {
        body [[string] | none]
        headers [[new line separated headers] | none]
        type [custom | default | redirect | soap-fault]
        url [[string] | none]
    }
edit profile [ [ [name] | [glob] | [regex] ] ... ]
    all-properties
    non-default-properties
```

Display

```
list profile
list profile [ [ [name] | [glob] | [regex] ] ... ]
show running-config profile
show running-config profile [ [ [name] | [glob] | [regex] ] ... ]
    all-properties
    non-default-properties
    one-line
    partition
    recursive
```

Delete

```
delete profile [name]
```

Description

You can use the **profile** component to create, modify, display, or delete an HTTP security profile for use with HTTP Protocol Security functionality.

Examples

create http my_http_profile defaults-from http_security

Creates a custom HTTP security named **my_http_profile** that inherits its settings from the system default HTTP security profile.

list profile

Displays the properties of all HTTP security profiles.

Options

- **app-service**
  Specifies the name of the application service to which the profile belongs. The default value is **none**. **Note:** If the **strict-updates** option is

enabled on the application service that owns the object, you cannot modify or delete the profile. Only the application service can modify or delete the profile.

- **[case-sensitive | case-insensitive]**
  Specifies whether the security profile treats file types as case sensitive, or not. The default value is **case-sensitive**. **Note:** If you create a profile, you can use either property, thereafter it becomes read only. If the security profile is case insensitive, the system stores file types in lowercase in the security profile configuration.
- **defaults-from**
  Specifies the profile that you want to use as the parent profile. Your new profile inherits all settings and values from the parent profile specified. The default value is **none**.
- **description**
  User defined description.
- **evasion-techniques**
  Specifies what action the system takes when it detects an evasion technique. Evasion techniques are methods used by attackers to avoid detection of their attack. You can configure the following options for evasion technique checks:
  - **alarm**
    Specifies, when enabled, that the system logs the request data and displays it in the Protocol Security Statistics screen whenever the system detects an evasion technique. The default value is **enabled**.
  - **block**
    Specifies, when enabled, that the system stops requests whenever the system detects an evasion technique. The default value is **disabled**.
- **file-types**
  Specifies which file types the security profile considers legal, and specifies what action the system takes when it detects a request for an illegal file type. You can configure the following options for file types:
  - **alarm**
    Specifies, when enabled, that the system logs the request data and displays it on the Protocol Security Statistics screen whenever the system detects a request for an illegal file type. The default value is **enabled**.
  - **[allowed | disallowed]**
    Indicates whether the **values** property lists file types that the security profile permits or prohibits. **Note:** For each security profile you may define either allowed file types or disallowed file types.
  - **block**
    Specifies, when enabled, that the system stops requests for an illegal file type. The default value is **disabled**.
  - **values**
    Adds, deletes, or replaces a set of file types considered either legal or illegal by the security profile. You can either select an available **file-type** or add a new one.

- **glob**
  Displays the items that match the **glob** expression. See **help glob** for a description of **glob** expression syntax.
- **http-rfc**
  Specifies which validations the system should check and what action the system takes when it detects a request that is not formatted properly. You can configure the following options for HTTP protocol checks:
  - **alarm**
    Specifies, when enabled, that the system logs the request data and displays it in the Protocol Security Statistics screen whenever a request fails one of the enabled HTTP protocol checks. The default value is **enabled**.
  - **bad-host-header**
    Specifies, when enabled, that the system inspects requests to see whether they contain a non RFC compliant header value. The default value is **enabled**.
  - **bad-version**
    Specifies, when enabled, that the system inspects requests to see whether they request information from a client using an HTTP protocol version 1.0 or higher. The default value is **enabled**.
  - **block**
    Specifies, when enabled, that the system stops requests whenever the system detects an evasion technique. The default value is **disabled**.
  - **body-in-get-head**
    Specifies, when enabled, that the system examines requests that use the HEAD or GET methods to see whether the requests contain data in their bodies, which is considered illegal. The default value is **disabled**.
  - **chunked-with-content-length**
    Specifies, when enabled, that the system examines chunked requests for a content-length header, which is not permitted. The default value is **enabled**.
  - **content-length-is-positive**
    Specifies, when enabled, that the system examines requests to see whether their content length value is greater than zero. The default value is **enabled**.
  - **header-name-without-value**
    Specifies, when enabled, that the system checks requests for valueless header names, which are considered illegal. The default value is **enabled**.
  - **high-ascii-in-headers**
    Specifies, when enabled, that the system inspects request headers for ASCII characters greater than 127, which are not permitted. The default value is **disabled**.
  - **host-header-is-ip**
    Specifies, when enabled, that the system verifies that the requestÐ¢¬Ä¬ôs host header value is not an IP address. The default value is **disabled**.

- **maximum-headers**
  Specifies whether the system compares the number of headers in the requests against the maximum number, and if so, how many headers are allowed. The default value is a maximum of **20** headers.
- **null-in-body**
  Specifies, when enabled, that the system inspects request bodies to see whether they contain a Null character, which is not allowed. The default value is **disabled**.
- **null-in-headers**
  Specifies, when enabled, that the system inspects request headers to see whether they contain a Null character, which is not allowed. The default value is **enabled**.
- **post-with-zero-length**
  Specifies, when enabled, that the system examines POST method requests for no content-length header, and for a content length of 0. The default value is **disabled**.
- **several-content-length**
  Specifies, when enabled, that the system examines each request to see whether it has more than one content-length header, which is considered illegal. The default value is **enabled**.
- **unparsable-content**
  Specifies, when enabled, that the system examines requests for content that the system cannot parse, which is not permitted. The default value is **enabled**.

◆ **mandatory-headers**
Specifies which headers must appear in requests, and specifies what action the system takes when it detects a request without a mandatory header. You can configure the following options for mandatory headers:

- **alarm**
  Specifies, when enabled, that the system logs the request data and displays it on the Protocol Security Statistics screen whenever a request does not include a mandatory header. The default value is **enabled**.
- **block**
  Specifies, when enabled, that the system stops requests that do not include a mandatory header. The default value is **disabled**.
- **values**
  Adds, deletes, or replaces a set of headers that must appear in requests to be considered legal by the security profile. You can either select an available **mandatory-header** or add a new one. **Note:** The system stores mandatory headers in lowercase in the security profile configuration, regardless of whether it is case sensitive or not.

◆ **maximum-length**
Specifies the default maximum length settings that the security profile considers legal, and specifies what action the system should take when it detects a request using an illegal length. You can configure the following options for length checks:

- **alarm**
  Specifies, when enabled, that the system logs the request data and displays it on the Protocol Security Statistics screen whenever a request fails one of the length checks. The default value is **enabled**.
- **block**
  Specifies, when enabled, that the system stops requests that fail one of the length checks. The default value is **disabled**.
- **post-data**
  Indicates whether there is a maximum acceptable length, in bytes, for the POST data portion of a request, and if so, specifies it. The default value is **any** (no restriction).
- **query-string**
  Indicates whether there is a maximum acceptable length, in bytes, for the query string portion of a request, and if so, specifies it. The default value is **1024** bytes.
- **request**
  Indicates whether there is a maximum acceptable length, in bytes, of a request, and if so, specifies it. The default value is **any** (no restriction).
- **uri**
  Indicates whether there is a maximum acceptable length, in bytes, for a URL, and if so, specifies it. The default value is **1024** bytes.

◆ **methods**
Specifies which HTTP methods the security profile considers legal, and specifies what action the system takes when it detects a request using an illegal method. You can configure the following options for methods:

- **alarm**
  Specifies, when enabled, that the system logs the request data and displays it on the Protocol Security Statistics screen whenever a request uses an illegal method. The default value is **enabled**.
- **block**
  Specifies, when enabled, that the system stops requests that use an illegal method. The default value is **disabled**.
- **values**
  Adds, deletes, or replaces a set of HTTP methods considered legal by the security profile. You can either select an available **asm http-method** or add a new one. **Note:** HTTP methods are case sensitive even if the security profile is case insensitive.

◆ **name**
Specifies a unique name for the component. This option is required for the commands **create**, **delete**, and **modify**.

◆ **partition**
Displays the administrative partition within which the component resides.

- **regex**
  Displays the items that match the regular expression. The regular expression must be preceded by an at sign (@[regular expression]) to indicate that the identifier is a regular expression. See **help regex** for a description of regular expression syntax.
- **response**
  Specifies information to display when the security profile blocks a client request. You can configure the following options for blocking page:
  - **body**
    Specifies the HTML code the system sends to the client in response to an illegal blocked request. Only if the response type is **custom**, you can edit this text.
  - **headers**
    Specifies the set of response headers that the system sends to the client in response to an illegal blocked request. Only if the response type is **custom**, you can edit this text. Separate each header with a new line (**Ctrl-V** followed by **Ctrl-J**).
  - **type**
    Specifies which content, or URL, the system sends to the client in response to an illegal blocked request.
    - **custom**
      Specifies a modified response text. You can edit the response header and HTML code in the properties **headers** and **body**.
    - **default**
      Specifies the system-supplied response text written in HTML. You cannot edit that text. This is the default value.
    - **redirect**
      Specifies that the system redirects the user to a specific web page instead of viewing a blocking page. You can edit the redirect web page in the **url** property.
    - **soap-fault**
      Specifies the system-supplied response written in SOAP fault message structure. You cannot edit that text. Use this type when a SOAP request is blocked due to an XML related violation.
  - **url**
    Specifies the particular URL to which the system redirects the user. Only if the response type is **redirect**, you can edit this text. The web page should include a full URL path, for example, **http://www.myredirectpage.com**.

See Also

http-method, *create*, *delete*, *edit*, glob, *list*, *virtual*, *modify*, regex, security, *security http*, *file-type*, *mandatory-header*, *tmsh*

87

security ip-intelligence

- Introducing the security ip-intelligence module
- Alphabetical list of components

Introducing the security ip-intelligence module

You can use these tmsh components to create firewall policies based on the IP Reputation of a packet's source. For example, you can create a rule to reject any packet whose source has an IP Reputation for phishing.

For more information about the tmsh hierarchical structure, see Chapter 2, *Understanding and Using the Traffic Management Shell*.

Alphabetical list of components

The remainder of this chapter lists the tmsh components that are available in the security ip-intelligence module.

blacklist-category

Global list of ip-intelligence blacklist categories. These ip-intelligence blacklist categories are used to configure ip-intelligence policies.

Syntax

Configure the **blacklist-category** component within the **security ip-intelligence** module using the syntax shown in the following sections.

Create/Modify

Display

```
list blacklist-category
show running-config blacklist-category
    all-properties
    non-default-properties
    one-line
    partition
    recursive
```

Description

You can use the **blacklist-category** component to configure a sharable and reusable blacklist category which can be configured with specific enforcement and logging settings under ip-intelligence policies.

Examples

modify blacklist-category Malware description "A variety of forms of hostile or intrusive software."

Modifies the blacklist-category description.

list blacklist-category

Displays the current list of blacklist categories.

Options

- **app-service**
  Specifies the application service to which the object belongs. The default value is **none**. **Note:** If the **strict-updates** option is **enabled** on the Application Service that owns the object, you cannot modify or delete the object. Only the Application Service can modify or delete the object.
- **description**
  User defined description.

- **partition**
  Displays the administrative partition within which the component resides.

See Also

create, *edit*, *list*, *modify*, *feed-list*, *policy*, *tmsh*

feed-list

Configures a feed-list for use by firewall. A *feed-list* is a list of URL feeds from where files are downloaded and the contents (IP-address prefixes) are compared against the source-IP address and/or destination-IP address in an IP packet by DWBL (Dynamic White/Black lists) by IP-Intelligence.

Syntax

Configure the **feed-list** component within the **security ip-intelligence** module using the syntax in the following sections.

Create/Modify

```
create feed-list [name]
modify feed-list [[name] | all]
  feeds [add | delete | modify | replace-all-with] {
    name [string] {
        default-blacklist-category [string]
        default-list-type [whitelist | blacklist]
        poll {
          interval [integer]
          user [string]
          url [string]
          password [string]
        }
      }
  }
  app-service [name]
  description [string]
edit feed-list [[name] | all]
    all-properties
    non-default-properties
load feed-list [[name] | all] feeds { name [string] }
```

Display

```
list feed-list [[name] | all | [property]]
show running-config feed-list [[name] | all | [property]]
    all-properties
    non-default-properties
    one-line
    partition
    recursive
```

Delete

```
delete feed-list [[name] | all]
```

Description

You can use the **feed-list** component to define reusable lists of feeds. You can use a feed list in a **security ip-intelligence policy**. A policy compares all of the addresses in the list (downloaded from a file at the specified url) to either the source or destination IP in the packet, depending on how you apply the list. If there is a match, the ip-intelligence policy takes an action, such as accepting or dropping the packet.

Examples

create feed-list alist1 feeds add { poll { url http://f5.com/bl.txt }

Creates a new feed list, "alist1," with IPv4/IPv6 addresses in the file downloaded from the specified url.

modify feed-list alist1 feeds modify { description "DWBL file from f5.com" }

Modifies the above feed list with a description.

modify feed-list alist1 feeds modify { poll { url https://f5.com/bl.txt }

Modifies the same feed by changing the protocol.

```
list feed-list alist1
security ip-intelligence feed-list alist1 {
   feeds {
       url2 {
           poll {
               url https://f5.com/bl.txt
               user user1
               password user1_pwd
           }
       }
       description "DWBL file from f5.com"
   }
}
```

Shows the modified feed list.

load feed-list alist1 alist2 feeds { feed1 feed2 }

Immediately downloads and updates feeds feed1 and feed2 of feed lists alist1 and alist2.

Options

- **feeds**
  Adds, deletes, or replaces feeds. You can configure the following options for a feed:
  - **name**
    Specifies a name for a feed. This option is required for the operations **create**, **delete**, **modify**, and **replace-all-with**.
  - **add**
    Creates a new feed list.

- **delete**
  Deletes the feed list that you specify next, in curly braces ({}).
- **modify**
  Makes it possible to replace the optional description(s) for the feed list.
- **replace-all-with**
  Replaces the current set of feed list with the a new one that you specify next, in curly braces ({}).
  - **default-list-type**
    Specifies a default type for this specific entry whether it is a blacklist or whitelist
  - **whitelist**
    Specifies that this entry is a whitelist.
  - **blacklist**
    Specifies that this entry is a blacklist.
  - **default-blacklist-category**
    Default blacklist category type for all blacklist entries that do not have a corresponding category string (eg. Botnet, Spyware, Malware)
  - **poll**
    You can configure the following options under this:
  - **interval**
    Specifies the frequency at which the url needs to be polled.
  - **user**
    Specifies the user which is used when downloading the url.
  - **url**
    Specifies the URL from where the white/black list will be downloaded. **Note:** Route domains are not supported when specifying the **url**.
  - **password**
    Password for the user.
- **default-list-type**
  Specifies a default type for this specific entry whether it is a blacklist or whitelist
  - **whitelist**
    Specifies that this entry is a whitelist.
  - **blacklist**
    Specifies that this entry is a blacklist.
- **app-service**
  Specifies the application service to which the object belongs. The default value is **none**. **Note:** If the **strict-updates** option is **enabled** on the Application Service that owns the object, you cannot modify or delete the object. Only the Application Service can modify or delete the object.

- **default-blacklist-category**
  Default blacklist category type for all blacklist entries that do not have a corresponding category string (eg. Botnet, Spyware, Malware)
- **description**
  User defined description for this feed list.
- **partition**
  Displays the administrative partition within which the component resides.

See Also

edit, *list*, *modify*, *self*, *route-domain*, *global-policy*, *security ip-intelligence*, *virtual*, *tmsh*

global-policy

Configures the global ip-intelligence policy. These ip-intelligence policy contents/filters are applied to all packets except those going through the management interface. They are applied first, before any firewall rules for the packet's virtual server, route domain.

Syntax

Modify the global-policy component within the **security ip-intelligence** module using the syntax shown in the following sections.

Modify

```
reset-stats global-policy
    ip-intelligence-categories
```

Display

```
list global-policy
show running-config global-policy
    all-properties
    non-default-properties
    one-line
    partition
    recursive
show global-policy
    ip-intelligence-categories
```

Description

You can use the **global-policy** component to configure a sharable and reusable set of network firewall DWBL (Dynamic White/Black lists) which can be enforced globally at the system level and the enforcement happens before the route-domain or virtual server level.

Examples

modify global-policy policy pol1

Modifies the global-policy with policy pol1.

list global-policy

Displays the current list of global-policy contents.

Options

- **app-service**
  Specifies the application service to which the object belongs. The default value is **none**. **Note:** If the **strict-updates** option is **enabled** on the Application Service that owns the object, you cannot modify or delete the object. Only the Application Service can modify or delete the object.
- **description**
  User defined description.
- **policy**
  Specifies an existing policy. **policy** contents are enforced at a global level.
- **partition**
  Displays the administrative partition within which the component resides.
- **ip-intelligence-categories**
  Used to show/ reset statistics on IP intelligence white/ black lists categories.

See Also

create, *edit*, *list*, *modify*, *feed-list*, *policy*, *tmsh*

info

Query IP Intelligence information about specified IP Address.

Syntax

Use the **info** component within the **security ip-intelligence** module to query IP Intelligence information about the IP address using the following syntax.

Display

```
show info address [IP address]
    virtual-server [name]
    route-domain [name]
```

Description

You can use the **info** component to query IP Intelligence information about an IP Address using IP Intelligence policy attached to the selected context. Global context is the default when the command is used without options. To select the virtual server or the route domain context use **virtual-server** or **route-domain** option. Only one option can be used. If the IP Address is listed in any of the DWBL (Dynamic White/Black List) feeds used by the selected IP Intelligence policy the query shows the list of categories and policy action (drop or allow) for the address. If the policy is configured to query legacy IP Reputation database, that information is also used in the query.

Examples

show info address 10.123.1.12

Query IP Intelligence information for IP address 10.123.1.12 using global IP Intelligence policy.

show info address 10.123.1.12 virtual-server /Commmon/vs

Query IP Intelligence information for IP address 10.123.1.12 using IP Intelligence policy configured for virtual server /Commmon/vs.

Options

- **virtual-server**
  Specifies the name of the virtual server configured with IP Intelligence poicy to use in the query. This option cannot be used with the **route-domain** option.

- **route-domain**
  Specifies the name of the route domain configured with IP Intelligence poicy to use in the query. This option cannot be used with the **virtual-server** option.

See Also

feed-list, *policy*, *tmsh*, *virtual*, *route-domain*

policy

Configures an ip-intelligence policy. It's comprised of three logical groups of settings: list of feed lists, enforcement and logging settings per blacklist category, and default enforcement and logging settings for blacklist categories.

Syntax

Configure the **policy** component within the **security ip-intelligence** module using the syntax in the following sections.

Create/Modify

Display

```
list policy [ [ [name] | [glob] | [regex] ] ... ]
show running-config policy
show running-config policy [ [ [name] | [glob] | [regex] ] ... ]
    all-properties
    non-default-properties
    one-line
    partition
    recursive
```

Description

You can use the **policy** component to configure a sharable and reusable enforcement and logging settings on Dynamic White/Black lists of IPs coming from downloaded feeds. The policy can then be enforced on a number of configuration objects of the following types: **ltm virtual**, **security ip-intelligence global-policy**, **net route-domain**.

Examples

```
create policy pol1 {
   blacklist-categories add {
    Spyware {
      action use-policy-setting
      app-service none
      description none
      log-blacklist-hit-only use-policy-setting
      log-blacklist-whitelist-hit yes
    }
   }
   feed-lists add { alist1 alist2 }
   default-action drop
   default-log-blacklist-hit-only yes
```

```
    default-log-blacklist-whitelist-hit no
    description none
    feed-lists none
    partition Common
}
```

Creates a policy pol1 with feeds from *alist1* and *alist2* feed lists, specific enforcement and logging settings for Spyware blacklist category and policy default settings for other categories.

modify policy pol1 { feed-lists delete { alist2 } }

Removes the feed-list alist2 from the policy pol1.

list policy

Displays the current list of ip-intelligence policies contents.

Options

- **app-service**
  Specifies the application service to which the object belongs. The default value is **none**. **Note:** If the **strict-updates** option is **enabled** on the Application Service that owns the object, you cannot modify or delete the object. Only the Application Service can modify or delete the object.
- **description**
  User defined description.
- **partition**
  Displays the administrative partition within which the component resides.
- **blacklist-categories**
  Adds, deletes, or replaces blacklist categories.
  - **action**
    Specifies what enforcement action will be applied if the packet is categorized with this blacklist category. If the packet is categorized with more than one blacklists the most restrictive action will be applied.
  - **log-blacklist-hit-only**
    Specifies if a log message will be generated if the packet is categorized with this blacklist and the packet's IP listed in no whitelists.
  - **log-blacklist-whitelist-hit**
    Specifies if a log message will be generated if the packet is categorized with this blacklist and the packet's IP is listed in a whitelist.
- **feed-lists**
  Adds, deletes, or replaces a feed list. Specifies a list of feed lists (see **security ip-intelligence feed-list**) against which the packet will be compared.

- **default-action**
  Specifies a default enforcement action which will be performed on the matched packet unless an implicit action specified for one of the blacklist categories the packet's IP is categorized with. If the packet's IP is listed in a white list the action is always *accept*.
- **default-log-blacklist-hit-only**
  Specifies a default blacklist hit only logging action which will be performed on the matched packet unless an implicit action specified for one of the blacklist categories the packet's IP is categorized with.
- **default-log-blacklist-whitelist-hit**
  Specifies a default blacklist and whitelist hit logging action which will be performed on the matched packet unless an implicit action specified for one of the blacklist categories the packet's IP is categorized with.

See Also

create, *edit*, *list*, *modify*, *feed-list*, *profile*, *tmsh*

88

security log

- Introducing the security log module
- Alphabetical list of components

Introducing the security log module

You can use the tmsh components that reside within the security log module to configure the Security Logging feature. For more information about the tmsh hierarchical structure, see Chapter 2, *Understanding and Using the Traffic Management Shell*.

Alphabetical list of components

The remainder of this chapter lists the tmsh components that are available in the security log module.

network-storage-field

Lists the available storage format fields that can be used in the context of Network Security Logging.

Syntax

Retrieve the list of the **network-storage-field** values using the syntax shown in the following sections.

Display

```
list network-storage-field
list network-storage-field [ [ [name] | [glob] | [regex] ] ... ]
    all
    all-properties
    one-line
    app-service
```

Description

Use this command to display the possible values of the **network-storage-field** object to be used in the context of Network Security Logging. These possible values are predefined traffic items available for the server to log in context of Network event logging (for example, ACL events, TCP Open/Close, TCP/IP error events).

Examples

list network-storage-field

Displays all the storage fields supported by Network Security Logging.

Options

- **app-service**
  Displays the application service to which the object belongs. The default value is **none**. **Note:** If the **strict-updates** option is **enabled** on the Application Service that owns the object, you cannot modify or delete the object. Only the Application Service can modify or delete the object.

See Also

glob, *list*, regex, *profile*, *tmsh*

profile

Configures a Security log profile.

Syntax

Configure the **profile** component within the **security log** module using the syntax shown in the following sections.

Create/Modify

```
create profile [name]
modify profile [name]
    app-service [[string] | none]
    application [none | add | delete | modify | replace-all-with] {
      name [string] {
          facility [local0 | local1 | local2 | local3 | local4 | local5 | local6 |
local7]
          filter [none | add | delete | modify | replace-all-with] {
            key [request-type | protocol | response-code | http-method |
                 search-all | search-in-headers | search-in-post-data |
search-in-query-string | search-in-request | search-in-uri] {
                values [none | add | delete | replace-all-with] { [string] ... }
            }
          }
          format {
            field-delimiter [string]
            field-format [string]
            fields [none | { [string] ... }]
            type [predefined | user-defined]
            user-string [string]
          }
          guarantee-logging [enabled | disabled]
          guarantee-response-logging [enabled | disabled]
          local-storage [enabled | disabled]
          logic-operation [and | or]
          maximum-entry-length [1k | 2k | 10k | 64k]
          maximum-header-size [integer]
          maximum-query-size [integer]
          maximum-request-size [integer]
          protocol [udp | tcp | tcp-rfc3195]
          remote-storage [none | remote | splunk | arcsight]
          report-anomalies [enabled | disabled]
          response-logging [none | illegal | all]
          servers [none | add | delete | modify | replace-all-with] {
            [IPv4:port | IPv6.port ... ]
          }
      }
    }
    description [string]
    dos-application [none | add | delete | modify | replace-all-with] {
      name [string] {
          local-publisher [name]
          remote-publisher [name]
    }
    ip-intelligence {
        aggregate-rate [integer]
```

```
        log-publisher [none | [name]]
        log-translation-fields [disabled | enabled]
    }
    traffic-statisticse {
        log-sctive-flows [disabled | enabled]
        log-publisher [none | [name]]
        log-missed-flows [disabled | enabled]
        log-reaped-flows [disabled | enabled]
        log-syncookies [disabled | enabled]
        log-syncookies-whitelist [disabled | enabled]
    }
    network [add | delete | modify | none | replace-all-with] {
      name [string] {
          filter {
            log-acl-match-accept [disabled | enabled]
            log-acl-match-drop [disabled | enabled]
            log-acl-match-reject [disabled | enabled]
            log-ip-errors [disabled | enabled]
            log-tcp-errors [disabled | enabled]
            log-tcp-events [disabled | enabled]
            log-translation-fields [disabled | enabled]
            log-geo-always [disabled | enabled]
          }
          rate-limit {
            acl-match-accept [integer]
            acl-match-drop [integer]
            acl-match-reject [integer]
            ip-errors [integer]
            tcp-errors [integer]
            tcp-events [integer]
            aggregate-rate [integer]
          }
          format {
            field-list [none | { acl_policy_name | acl_policy_type | acl_rule_name |
action | bigip_hostname | context_name | context_type | date_time |
                        dest_ip | dest_port | drop_reason | management_ip_address |
protocol | route_domain |
                      sa_translation_pool | sa_translation_type | src_ip | src_port |
translated_dest_ip |
                        translated_dest_port | translated_ip_protocol |
translated_route_domain |
                        translated_src_ip | translated_src_port | translated_vlan |
vlan }]
            field-list-delimiter [string]
            type [field-list | none | user-defined]
            user-defined [string]
          }
          publisher [none | [name]]
      }
    }
    protocol-dns [add | delete | modify | none | replace-all-with] {
      name [string] {
          filter {
            log-dns-drop [disabled | enabled]
            log-dns-filtered-drop [disabled | enabled]
            log-dns-malformed [disabled | enabled]
            log-dns-malicious [disabled | enabled]
            log-dns-reject [disabled | enabled]
          }
          format {
            field-list [none | { action | attack_type | context_name | date_time |
dest_ip | dest_port |
```

```
                        dns_query_name | dns_query_type | src_ip | src_port | vlan |
route_domain }]
            field-list-delimiter [string]
            type [field-list | none | user-defined]
            user-defined [string]
          }
          publisher [none | [name]]
      }
    }
    protocol-dns-dos-publisher [none | [name]]
    protocol-sip [add | delete | modify | none | replace-all-with] {
      name [string] {
          filter {
            log-sip-drop [disabled | enabled]
            log-sip-global-failures [disabled | enabled]
            log-sip-malformed [disabled | enabled]
            log-sip-redirection-responses [disabled | enabled]
            log-sip-request-failures [disabled | enabled]
            log-sip-server-errors [disabled | enabled]
          }
          format {
            field-list [none | { action | attack_type | context_name | date_time |
dest_ip | dest_port |
                       sip_method_type | sip_caller | sip_callee | src_ip | src_port |
vlan | route_domain }]
            field-list-delimiter [string]
            type [field-list | none | user-defined]
            user-defined [string]
          }
          publisher [none | [name]]
      }
    }
    protocol-sip-dos-publisher [none | [name]]
    dos-network-publisher [none | [name]]
    protocol-transfer [none | add | delete | modify | replace-all-with] {
      name [string] {
          publisher [name]
    }
edit profile [ [ [name] | [glob] | [regex] ] ... ]
    all-properties
    non-default-properties
```

Display

```
list profile
list profile [ [ [name] | [glob] | [regex] ] ... ]
show running-config profile
show running-config profile [ [ [name] | [glob] | [regex] ] ... ]
    all-properties
    non-default-properties
    one-line
    partition
    recursive
```

Delete

```
delete profile [name]
```

Description

You can use the **profile** component to create, modify, display, or delete a Security log profile for use with Security Logging functionality.

Examples

create profile my_log_profile

Creates a custom Security log profile named **my_log_profile** with initial settings.

list profile

Displays the properties of all Security log profiles.

Options

- **app-service**
  Specifies the name of the application service to which the profile belongs. The default value is **none**. **Note:** If the **strict-updates** option is **enabled** on the application service that owns the object, you cannot modify or delete the profile. Only the application service can modify or delete the profile.
- **application**
  Adds, deletes, or replaces a single Application Security sub-profile. You can configure the following options for Application Security:
  - **facility**
    Specifies the facility category of the logged traffic in Application Security. Select between **local0** and **local7**.
  - **filter**
    Adds, deletes, or replaces a set of request filters in Application Security. You can configure the following options for a request filter:
    - **key**
      Specifies a unique key for the request filter. This option is required for the operations **create**, **delete**, **modify**, and **replace-all-with**. The options are:
      - **request-type**
        Specifies which kind of requests the system, or server, logs.
      - **protocol**
        Specifies whether request logging is dependent on the protocol.
      - **response-code**
        Specifies whether request logging is dependent on the response status code.
      - **http-method**
        Specifies whether request logging is dependent on the HTTP method.

- **search-all**, **search-in-headers**, **search-in-post-data**, **search-in-query-string**, **search-in-request**, **search-in-uri**
  Specifies whether the request logging is dependent on a specific string, and if so, the part of the request where the system must find the string. You can select only one of these filters, the default is **search-all**, which means that the system logs all requests, regardless of string.
- **values**
  Adds, deletes, or replaces a set of values in the request filter.

- **format**
  Specifies a storage format in Application Security. You can configure the following options for the storage format:
  - **field-delimiter**
    Specifies a field delimiter in the **predefined** storage format. You may not use the % character. The default delimiter is the comma character, for CSV.
  - **field-format**
    Specifies a field format (for each key/value pair) in the **predefined** storage format. Use %k for key and %v for value. The default format is empty that is interpreted as "%v", for CSV.
  - **fields**
    Replaces a set of fields in the **predefined** storage format. The order in the set is important - the server displays the selected traffic items in the log sequentially according to it.
  - **type**
    Specifies a type of the storage format. The options are:
    - **predefined**
      Specifies that the log displays only the predefined items you select in the **fields**.
    - **user-defined**
      Specifies that the log displays any free text that you type in the **user-string** which can include the predefined items.
  - **user-string**
    Specifies a user string in the **user-defined** storage format.
- **guarantee-logging**
  Indicates whether to guarantee local logging in Application Security.
- **guarantee-response-logging**
  Indicates whether to guarantee local response logging in Application Security. In order to enable it, you must first enable **guarantee-logging**, and set **response-logging** to either **illegal** or **all**.
- **local-storage**
  Enables or disables local storage in Application Security.
- **logic-operation**
  Specifies the logic operation on the associated filters in Application Security. The options are:

- **and**
  Specifies that requests must pass all filters in order for the system, or server, to log the requests.
- **or**
  Specifies that requests must meet at least one filter in order for the system, or server, to log the requests. This is the default value.

- **maximum-entry-length**
  Specifies the maximum entry length in Application Security. The options are:
  - **1k**
    This is the default length for remote servers that support the **udp** protocol.
  - **2k**
    This is the default length for remote servers that support the **tcp** and **tcp-rfc3195** protocols.
  - **10k**, **64k**
    These are possible lengths for remote servers that support the **tcp** protocol.
- **maximum-header-size**
  Specifies the maximum headers size in Application Security.
- **maximum-query-size**
  Specifies the maximum query string size in Application Security.
- **maximum-request-size**
  Specifies the maximum request size in Application Security.
- **name**
  Specifies a dummy name for enabled Application Security. This option is required for the operations **create**, **delete**, **modify**, and **replace-all-with**.
- **protocol**
  Specifies the protocol supported by the remote server in Application Security. Select either: **tcp** (the default value), **udp**, or **tcp-rfc3195**.
- **remote-storage**
  Specifies a remote storage type in Application Security. The options are:
  - **none**
    Specifies that the system does not store traffic on any remote logging server.
  - **remote**
    Specifies that the system stores all traffic on a remote logging server, like a syslog.
  - **splunk**
    Specifies that the system stores all traffic on a reporting server (Splunk) using a preconfigured storage format. Key/value pairs are used in the log messages.

- **arcsight**
  Specifies that the system stores all traffic on a remote logging server using the predefined ArcSight settings for the logs. The log messages are in Common Event Format (CEF).

- **report-anomalies**
  Indicates whether to report detected anomalies in Application Security.

- **response-logging**
  Specifies a response logging type in Application Security. The options are:

  - **none**
    Specifies that the system does not log responses. This is the default value.

  - **illegal**
    Specifies that the system logs responses to illegal requests.

  - **all**
    Specifies that the system logs all responses if the associated **request-type** filter has the **all** value.

- **servers**
  Adds, deletes, or replaces a set of remote servers in Application Security, by specifying an IP address and service port in the format **[IPv4:port]** or **[IPv6.port]**.

◆ **description**
User defined description.

◆ **dos-application**
Adds, deletes, or replaces a single DoS (Application) Protection sub-profile. You can configure the following options for DoS (Application) Protection:

- **local-publisher**
  Specifies the name of the local log publisher used for Application DoS attacks. **Note:** This publisher should have a single **local-database** destination.

- **name**
  Specifies a dummy name for enabled DoS (Application) Protection. This option is required for the operations **create**, **delete**, **modify**, and **replace-all-with**.

- **remote-publisher**
  Specifies the name of the remote log publisher used for Application DoS attacks. **Note:** This publisher should have either **arcsight** or **splunk** destinations.

◆ **glob**
Displays the items that match the **glob** expression. See **help glob** for a description of **glob** expression syntax.

◆ **ip-intelligence**
You can configure the following options under this:

- **aggregate-rate**
  This option is used to set the aggregate rate limit that applies to any ip intelligence log message.
- **log-publisher**
  Specifies the name of the log publisher used for IP Intelligence events.
- **log-translation-fields**
  This option is used to enable or disable the logging of translated (i.e server side) fields in IP Intelligence log messages. Translated fields include (but not limited to) Source Address/Port, Destination Address/Port, IP Protocol, Route Domain and Vlan.

◆ **traffic-statistics**
You can configure the following options under this:

- **log-active-flows**
  This option is used to enable and disable the logging of number of active flows on client side. The number of flows are logged globally, per virtual server and per route domain periodically if number of active flows increased or decreased.
- **log-publisher**
  Specifies the name of the log publisher used for Traffic Statistics logs.
- **log-reaped-flows**
  This option is used to enable and disable the logging of number of reaped flows on client side. The number of flows are logged globally, per virtual server and per route domain periodically if number of active flows increased or decreased.
- **log-missed-flows**
  This option is used to enable and disable the logging of number of TCP packets (non SYN/ACK) were dropped because of the flow table lookup failed. The number of packets are logged globally, and per route domain periodically.
- **log-syncookies**
  This option is used to enable and disable the logging of number of syncookies generated, accepted and rejected in the context globally and per virtual server. These log messages will be generated periodically.
- **log-syncookies-whitelist**
  This option is used to enable and disable the logging of number of syncookies whitelist hits, accepted and rejected in the context globally and per virtual server. These log messages will be generated periodically.

◆ **network**
Add, delete, modify or replace a single Network Security sub-profile. You can configure the following options under this:

- **filter**
  Following options are available which enable or disable the logging of corresponding Network events:

- **log-acl-match-accept**
  This option is used to enable or disable the logging of packets that match ACL rules configured with action = Accept or action = Accept Decisively.
- **log-acl-match-drop**
  This option is used to enable or disable the logging of packets that match ACL rules configured with action = Drop.
- **log-acl-match-reject**
  This option is used to enable or disable the logging of packets that match ACL rules configured with action = Reject.
- **log-ip-errors**
  This option is used to enable or disable the logging of IP error packets.
- **log-tcp-errors**
  This option is used to enable or disable the logging of TCP error packets.
- **log-tcp-events**
  This option is used to enable or disable the logging of TCP events on client side. Only ‘Established’ and ‘Closed’ states of a TCP session are logged if this option is enabled.
- **log-translation-fields**
  This option is used to enable or disable the logging of translated (i.e server side) fields in ACL match and TCP events. Translated fields include (but not limited to) Source Address/Port, Destination Address/Port, IP Protocol, Route Domain and Vlan.
- **log-geo-always**
  This option is used to enable or disable the logging of Geographic IP Location information fields in ACL match and TCP logging. Geographic information includes the country code of Source Address and Destination Address.

- **rate-limit**
  Following options are available to set throttling rate limits for the corresponding logging network events:
  - **acl-match-accept**
    This option is used to set rate limits for the logging of packets that match ACL rules configured with action = Accept or action = Accept Decisively. This option is effective only if logging of this message type is enabled.
  - **acl-match-drop**
    This option is used to set rate limits for the logging of packets that match ACL rules configured with action = Drop. This option is effective only if logging of this message type is enabled.
  - **acl-match-reject**
    This option is used to set rate limits for the logging of packets that match ACL rules configured with action = Reject. This option is effective only if logging of this message type is enabled.

- **ip-errors**
  This option is used to set rate limits for the logging of IP error packets. This option is effective only if logging of this message type is enabled.
- **tcp-errors**
  This option is used to set rate limits for the logging of TCP error packets. This option is effective only if logging of this message type is enabled.
- **tcp-events**
  This option is used to set rate limits for the logging of TCP events on client side. This option is effective only if logging of this message type is enabled.
- **aggregate-rate**
  This option is used to set the aggregate rate limit that applies to any network loggging message.

- **format**
  Specifies the Storage format in Network Security sub-profile. These settings are only used to format the log messages destined to a Remote Syslog server. You can configure the following options for the storage format:
  - **field-list**
    Specifies a set of fields to be logged. This option is valid when storage format type is **field-list**. The order in the set is important - the server displays the selected traffic items in the log sequentially according to it. User can pick fields from the following list: **acl_policy_name**, **acl_policy_type**, **acl_rule_name**, **action**, **bigip_hostname**, **context_name**, **context_type**, **date_time**, **dest_ip**, **dest_port**, **drop_reason**, **management_ip_address**, **protocol**, **route_domain**, **sa_translation_pool**, **sa_translation_type**, **src_ip**, **src_port**, **translated_dest_ip**, **translated_dest_port**, **translated_ip_protocol**, **translated_route_domain**, **translated_src_ip**, **translated_src_port**, **translated_vlan**, **vlan**.
  - **field-list-delimiter**
    Specifies the delimiter string in **field-list** storage format type. The default delimiter is the comma character, for CSV. This option is valid when storage format type is **field-list**. Special character **$** should not be used in delimiter string as it is reserved for internal usage. Also, the maximum length allowed for **field-list-delimiter** is 31 characters (excluding NUL terminator).
  - **type**
    Specifies a type of the storage format. The options are:
    - **field-list**
      Specifies that the log displays only the items you specify in the **field-list** with **field-list-delimiter** as the delimiter between the items.

- **none**
  Default format type. With this option, the messages will be logged in the following format: "management_ip_address","bigip_hostname","context_type","context_name","src_ip","dest_ip","src_port","dest_port","vlan","protocol","route_domain","translated_src_ip","translated_dest_ip","translated_src_port","translated_dest_port","translated_vlan","translated_ip_protocol","translated_route_domain","acl_policy_type","acl_policy_name","acl_rule_name","action","drop_reason","sa_translation_type","sa_translation_pool"
- **user-defined**
  Specifies that the log displays the message as per the **user-defined** string format.

- **user-defined**
  Specifies the format of log message in form of user defined string. This option is valid when storage format type is **user-defined**. Maximum configurable length is 512 characters. Any of the following items, if wrapped within ${ }, will be substituted with the actual value when generating the log: **acl_policy_type**, **acl_policy_name**, **acl_rule_name**, **action**, **bigip_hostname**, **context_name**, **context_type**, **date_time**, **dest_ip**, **dest_port**, **drop_reason**, **management_ip_address**, **protocol**, **route_domain**, **sa_translation_pool**, **sa_translation_type**, **src_ip**, **src_port**, **translated_dest_ip**, **translated_dest_port**, **translated_ip_protocol**, **translated_route_domain**, **translated_src_ip**, **translated_src_port**, **translated_vlan**, **vlan**.
- **publisher**
  Specifies the name of the log publisher used for Network events.

◆ **name**
Specifies a unique name for the component. This option is required for the commands **create**, **delete**, and **modify**.

◆ **partition**
Displays the administrative partition within which the component resides.

◆ **protocol-dns**
Add, delete, modify or replace a single Protocol (DNS) Security sub-profile. You can configure the following options under this:

- **filter**
  Following options are available which enable or disable the logging of corresponding Network events:
  - **log-dns-drop**
    This option is used to enable or disable the logging of dropped DNS packets.
  - **log-dns-filtered-drop**
    This option is used to enable or disable the logging of DNS packets that are dropped due to filtering.

- **log-dns-malformed**
  This option is used to enable or disable the logging of malformed DNS packets.
- **log-dns-malicious**
  This option is used to enable or disable the logging of malicious DNS packets.
- **log-dns-reject**
  This option is used to enable or disable the logging of rejected DNS packets.

- **format**
  Specifies the Storage format in Protocol (DNS) Security sub-profile. These settings are only used to format the log messages destined to a Remote Syslog server. You can configure the following options for the storage format:
  - **field-list**
    Specifies a set of fields to be logged. This option is valid when storage format type is **field-list**. The order in the set is important - the server displays the selected traffic items in the log sequentially according to it. User can pick fields from the following list: **action**, **attack_type**, **context_name**, **date_time**, **dest_ip**, **dest_port**, **dns_query_name**, **dns_query_type**, **src_ip**, **src_port**, **vlan**.
  - **field-list-delimiter**
    Specifies the delimiter string in **field-list** storage format type. The default delimiter is the comma character, for CSV. This option is valid when storage format type is **field-list**. Special character **$** should not be used in delimiter string as it is reserved for internal usage. Also, the maximum length allowed for **field-list-delimiter** is 31 characters (excluding NUL terminator).
  - **type**
    Specifies a type of the storage format. The options are:
    - **field-list**
      Specifies that the log displays only the items you specify in the **field-list** with **field-list-delimiter** as the delimiter between the items.
    - **none**
      Default format type. With this option, the messages will be logged in the following format:
      "date_time","context_name","vlan","dns_query_type","dns_query_name",
      "attack_type","action","src_ip","dest_ip","src_port","dest_port", "route_domain"
    - **user-defined**
      Specifies that the log displays the message as per the **user-defined** string format.
  - **user-defined**
    Specifies the format of log message in form of user defined string. This option is valid when storage format type is **user-defined**. Maximum configurable length is 512 characters. Any of the

following items, if wrapped within ${ }, will be substituted with the actual value when generating the log: **action**, **attack_type**, **context_name**, **date_time**, **dest_ip**, **dest_port**, **dns_query_name**, **dns_query_type**, **route_domain**, **src_ip**, **src_port**, **vlan**.

- **name**
  Specifies a dummy name for enabled Protocol (DNS) Security. This option is required for the operations **create**, **delete**, **modify**, and **replace-all-with**.
- **publisher**
  Specifies the name of the log publisher used for DNS events.

◆ **protocol-dns-dos-publisher**
Specifies the name of the log publisher used for DNS DoS events.

◆ **dos-network-publisher**
Specifies the name of the log publisher used for DoS Network events.

◆ **protocol-sip**
Add, delete, modify or replace a single Protocol (SIP) Security sub-profile. You can configure the following options under this:

- **filter**
  Following options are available which enable or disable the logging of corresponding protocol sip events:
  - **log-sip-drop**
    This option is used to enable or disable the logging of dropped SIP packets.
  - **log-sip-global-failures**
    This option is used to enable or disable the logging of SIP packets that resulted in global failures.
  - **log-sip-malformed**
    This option is used to enable or disable the logging of malformed SIP packets.
  - **log-sip-redirection-responses**
    This option is used to enable or disable the logging of SIP packets that resulted in sending redirection response.
  - **log-sip-request-failures**
    This option is used to enable or disable the logging of SIP request failures.
  - **log-sip-server-errors**
    This option is used to enable or disable the logging of SIP packets that resulted in server errors.
- **format**
  Specifies the Storage format in Protocol (SIP) Security sub-profile. These settings are only used to format the log messages destined to a Remote Syslog server. You can configure the following options for the storage format:
  - **field-list**
    Specifies a set of fields to be logged. This option is valid when storage format type is **field-list**. The order in the set is important - the server displays the selected traffic items in the log sequentially

according to it. User can pick fields from the following list: **action**, **attack_type**, **context_name**, **date_time**, **dest_ip**, **dest_port**, **dns_query_name**, **dns_query_type**, **src_ip**, **src_port**, **vlan**.

- **field-list-delimiter**
  Specifies the delimiter string in **field-list** storage format type. The default delimiter is the comma character, for CSV. This option is valid when storage format type is **field-list**. Special character **$** should not be used in delimiter string as it is reserved for internal usage. Also, the maximum length allowed for **field-list-delimiter** is 31 characters (excluding NUL terminator).
- **type**
  Specifies a type of the storage format. The options are:
  - **field-list**
    Specifies that the log displays only the items you specify in the **field-list** with **field-list-delimiter** as the delimiter between the items.
  - **none**
    Default format type. With this option, the messages will be logged in the following format:
    "date_time","context_name","vlan","sip_method_type","sip_caller", "sip_callee",
    "attack_type","action","src_ip","dest_ip","src_port","dest_port", "route_domain"
  - **user-defined**
    Specifies that the log displays the message as per the **user-defined** string format.
- **user-defined**
  Specifies the format of log message in form of user defined string. This option is valid when storage format type is **user-defined**. Maximum configurable length is 512 characters. Any of the following items, if wrapped within ${ }, will be substituted with the actual value when generating the log: **action**, **attack_type**, **context_name**, **date_time**, **dest_ip**, **dest_port**, **dns_query_name**, **dns_query_type**, **route_domain**, **src_ip**, **src_port**, **vlan**.

- **name**
  Specifies a dummy name for enabled Protocol (SIP) Security. This option is required for the operations **create**, **delete**, **modify**, and **replace-all-with**.
- **publisher**
  Specifies the name of the log publisher used for SIP events.

◆ **protocol-sip-dos-publisher**
Specifies the name of the log publisher used for SIP DoS events.

◆ **protocol-transfer**
Adds, deletes, or replaces a single Protocol (Transfer) Security sub-profile. You can configure the following options for Protocol (Transfer) Security:

- **name**
  Specifies a dummy name for enabled Protocol (Transfer) Security. This option is required for the operations **create**, **delete**, **modify**, and **replace-all-with**.
- **publisher**
  Specifies the name of the log publisher used for Protocol Security log messages. **Note:** This publisher should have either **local-database**, **local-syslog**, **remote-syslog**, **arcsight** or **splunk** single destination.

◆ **regex**
Displays the items that match the regular expression. The regular expression must be preceded by an at sign (@[regular expression]) to indicate that the identifier is a regular expression. See **help regex** for a description of regular expression syntax.

See Also

http-method, *response-code*, *create*, *delete*, *edit*, glob, *list*, *virtual*, *modify*, regex, security, *security log*, *storage-field*, *show*, *sys log-config destination*, *publisher*, *tmsh*

protocol-dns-storage-field

Lists the available storage format fields that can be used in the context of Protocol DNS Security Logging.

Syntax

Retrieve the list of the **protocol-dns-storage-field** values using the syntax shown in the following sections.

Display

```
list protocol-dns-storage-field
list protocol-dns-storage-field [ [ [name] | [glob] | [regex] ] ... ]
    all
    all-properties
    one-line
    app-service
```

Description

Use this command to display the possible values of the **protocol-dns-storage-field** object to be used in the context of Protocol DNS Security Logging. These possible values are predefined traffic items available for the server to log in the context of DNS event logging (for example, Malformed, Malicious, or Dropped DNS packets).

Examples

list protocol-dns-storage-field

Displays all the storage fields supported by Protocol DNS Security Logging.

Options

- **app-service**
  Displays the application service to which the object belongs. The default value is **none**. **Note:** If the **strict-updates** option is **enabled** on the Application Service that owns the object, you cannot modify or delete the object. Only the Application Service can modify or delete the object.

See Also

glob, *list*, regex, *profile*, *tmsh*

protocol-sip-storage-field

Lists the available storage format fields that can be used in the context of Protocol SIP Security Logging.

Syntax

Retrieve the list of the **protocol-sip-storage-field** values using the syntax shown in the following sections.

Display

```
list protocol-sip-storage-field
list protocol-sip-storage-field [ [ [name] | [glob] | [regex] ] ... ]
    all
    all-properties
    one-line
    app-service
```

Description

Use this command to display the possible values of the **protocol-sip-storage-field** object to be used in the context of Protocol SIP Security Logging. These possible values are predefined traffic items available for the server to log in the context of SIP event logging (e.g Dropped SIP packets).

Examples

list protocol-sip-storage-field

Displays all the storage fields supported by Protocol SIP Security Logging.

Options

- **app-service**
  Displays the application service to which the object belongs. The default value is **none**. **Note:** If the **strict-updates** option is **enabled** on the Application Service that owns the object, you cannot modify or delete the object. Only the Application Service can modify or delete the object.

See Also

glob, *list*, regex, *profile*, *tmsh*

remote-format

Lists the log format for different remote destinations (such as ArcSight, Splunk etc.) used by various Firewall events (such as Network, IP Intelligence, DoS etc.).

Syntax

Retrieve the list of the **remote-format** using the syntax shown in the following sections.

Display

```
list remote-format
list remote-format [ [ [name] | [glob] | [regex] ] ... ]
    all
    all-properties
    app-service
    format
    one-line
```

Description

Use this command to display the actual log format used to send firewall event logs to remote destinations such as ArcSight, Splunk and Syslog. These log formats are used by the log destinations of log publisher configured in different sub-profiles (for example Network, IP Intelligence, DNS, DNS DoS etc.) of a **security log profile**.

Examples

list remote-format

Displays the log format for all firewall events.

list remote-format network-arcsight

Displays the format for Network log events (such as ACL matches, TCP events etc.) sent to an ArcSight destination.

list remote-format network-dos-splunk

Displays the format for Network DoS log events sent to a Splunk destination.

list remote-format ip-intelligence-syslog-default

Displays the format for IP Intelligence log events sent to a remote syslog destination.

Options

- **app-service**
  Displays the application service to which the object belongs. The default value is **none**. **Note:** If the **strict-updates** option is **enabled** on the Application Service that owns the object, you cannot modify or delete the object. Only the Application Service can modify or delete the object.
- **format**
  Displays the remote log format used by the object.

See Also

glob, *list*, regex, *profile*, *tmsh*

storage-field

Lists the available storage format fields that can be used in the context of Application Security Logging.

Syntax

Retrieve the list of the **storage-field** values using the syntax shown in the following sections.

Display

```
list storage-field
list storage-field [ [ [name] | [glob] | [regex] ] ... ]
    all
    app-service
    format
    id
    one-line
```

Description

Use this command to display the possible values of the storage-field object to be used in the context of Application Security Logging. These possible values are predefined traffic items available for the server to log. The traffic items appear in the final format string as arguments in the **printf** () function, i.e. "%<position>$<specifier>", therefore each storage field has its fixed format (specifier) and id (position).

Examples

list storage-field

Displays all the storage fields supported by Application Security Logging.

Options

- **app-service**
  Displays the application service to which the object belongs. The default value is **none**. **Note:** If the **strict-updates** option is **enabled** on the Application Service that owns the object, you cannot modify or delete the object. Only the Application Service can modify or delete the object.
- **format**
  Displays a format of the field (s - string, d - decimal). It corresponds to the conversion specifier in the **printf** () function.

- **id**
  Displays an order ID of the field (starting from 1). It corresponds to the position in the argument list of the desired argument in the **printf** () function.

See Also

glob, *list*, regex, *profile*, *tmsh*

89

sys

- Introducing the sys module
- Alphabetical list of components

Introducing the sys module

You can use the tmsh components that reside within the sys module to configure the BIG-IP® system settings and display information about the system. For more information about the tmsh hierarchical structure, see Chapter 2, *Understanding and Using the Traffic Management Shell*.

Alphabetical list of components

The remainder of this chapter lists the tmsh components that are available in the sys module.

clock

Displays the current date and time.

Syntax

Display

```
show clock
    field-fmt
modify clock
    time [time]
```

Description

You can use the **clock** component to display the system date and time.

Examples

show clock

Display the current date and time.

modify clock time 2012-12-11:12:30:45

Set the system clock to the specified time.

Options

For information about the options that you can use with the command **show**, see **help show**.

See Also

show, *tmsh*

cluster

Configures a cluster in a VIPRION® system.

Syntax

Configure the **cluster** component within the **sys** module using the syntax in the following sections.

Modify

```
modify cluster [name]
    address [IP address | none]
    members {
      [1 | 2 | 3 | 4] {
          address [IP address | none]
          [disabled | enabled]
          priming [disabled | enabled]
      }
    }
    min-up-members [integer]
    min-up-members-enabled [no | yes]
edit cluster default
    all-properties
    non-default-properties
```

Display

```
list cluster
show running-config cluster
show running-config cluster [option name]
    one-line
show cluster
show cluster [option name]
    field-fmt
```

Description

You can use the **cluster** component to modify the configuration of the primary blade in a cluster. When you do this, the system automatically propagates the changes to the other blades in the cluster. This is known as cluster synchronization.

Examples

modify cluster default address 192.168.217.44/24

Sets the floating management IP address for the cluster **default** to an IP address of **192.168.217.44**.

list cluster my_cluster

Displays the properties of the cluster named **my_cluster**.

Options

address

Specifies an IP address for the cluster or cluster member. The default value is **none**.

disabled

Disables the specified cluster member. The default value is **enabled**.

enabled

Enables the specified cluster member. This is the default value.

members

Specifies the cluster members to be acted on by the command. A cluster member is a slot into which you insert a blade. The cluster member is identified by the number assigned to the slot.

min-up-members

Specifies the minimum number of cluster members that must be up for the cluster to remain Active. The default value is **1**.

min-up-members-enabled

When set to **yes**, specifies that when the number of cluster members that are active is below the value of the option **min-upmembers**, the cluster fails over to its peer. The default value is **no**.

Enable this parameter when you configure a redundant pair.

Important

*Make sure that you modify the value of the **min-up-members** option appropriately when you take blades down in a cluster. Otherwise, you can get into the condition where disabling a cluster member brings the cluster below the value of the option **min-up-members**, which can cause the cluster to fail over to its peer.*

name

Specifies a name for the cluster. This option is required.

priming

Prevents a cluster member from proceeding to the RUNNING cluster quorum state, which is useful when a blade is in a reboot loop. The default value is **disabled**.

See Also

edit, *list*, *modify*, *show*, *tmsh*

config

Manages the BIG-IP® system configuration.

Syntax

Save the running configuration or load the system configuration files within the **sys** module using the following syntax.

Modify

```
save config
    base
    binary
    current-partition
    exclude-gtm
    file
    gtm-only
    one-line
    passphrase
    partitions
    tar-file
    time-stamp
    user-only
    wait
load config
    base
    current-partition
    default
    exclude-gtm
    file
    files-folder
    from-terminal
    gtm-only
    merge
    passphrase
    partitions
    tar-file
    user-only
    verify
delete config file [file name]
```

Display

```
list config file
```

Description

The system applies all configuration changes that you make from within **tmsh** to the running configuration. To save the running configuration to the system configuration files, use the command sequence **save config**.

Additionally, you can replace the running configuration with the configuration in the system configuration files using the command sequence **load config**.

If any of these options are not specified, **save/load config** will save or load the configuration in all partitions on this system:

- **binary**
- **default**
- **file**
- **from-terminal**
- **partitions**

Examples

save config

Saves the running configuration in all partitions by overwriting the system configuration files.

In Virtual Editions with **f5-swap-eth** installed, saves the mapping of Ethernet device names and MAC addresses to **/etc/ethmap** to make the working BIG-IP still work after adding/deleting virtual NIC(s). It also works for **save config partitions all**.

save config base

Saves the running base configuration in all partitions by overwriting the system base configuration files.

save config binary

Saves all running configuration by overwriting the system binary configuration database file.

save config current-partition

Saves the running configuration in current update partition by overwriting the system configuration files.

save config wait

Save request waits if another save operation is in progress.

save config file my_file tar-file my_tar_file

Saves all running configuration to the specified file, **my_file**, and all the user provided disk files referred to by the configuration into **my_tar_file**.

save config file my_file passphrase my_password

Saves all running configuration to the specified file, **my_file** and encrypt it with **my_password**.

save config partitions { my_partition }

Saves the running configuration in **my_partition** by overwriting the system configuration files.

save config partitions all

Saves the running configuration in all partitions by overwriting the system configuration files.

save config user-only

Saves only user account configuration by overwriting the system configuration files.

load config

Replaces the running configuration in all partitions with the configuration in the system configuration files.

load config base

Replaces the running base configuration in the all partitions with the configuration in the system base configuration files.

load config current-partition

Replaces the running configuration in current update partition with the configuration in the system configuration files.

load config merge file my_file

Loads the specified configuration from my_file, which modifies the running configuration.

load config verify file my_file

Validates the specified configuration in my_file to see whether they are valid to replace the running configuration. The running configuration will not be changed.

load config verify merge file my_file

Validates the specified configuration in my_file to see whether they are valid to be merged into the running configuration. The running configuration will not be changed.

load config default

Sets system configuration back to factory default settings.

load config file my_file tar-file my_tar_file

Replaces all running configurations with the configuration in the specified file, **my_file** and the disk files referred to by the configuration are retrieved from **my_tar_file**.

load config file my_file files-folder my_files_folder

Replace all running configuration with the configuration in the specified file, **my_file** and the disk files referred to by the configuration is taken from the directory tree under **my_files_folder**.

load config file my_file passphrase my_password

Replaces all running configuration with the configuration in the specified encrypted file, **my_file** and decrypt it with **my_password**.

While searching for disk files under the specified folder, the order of search is first by file name as in cache-path, and then by object-name. If more than one file is found for a name, then the relative path in the cache-path is used to make the selection.

That is, while looking for
<Bsys file ssl-cert xxx {
cache-path /config/filestore/files_d/Common_d/certificate_d/xxx_1
...
}>

Looks for file(s) named B<xxx_1>.
If none are found, looks for file(s) named "xxx"

When more than one file is found, looks for a copy that matches paths in the order:
B<certificate_d/<name-found>>
B<Common_d/certificate_d/<name-found>>

load config partitions { x }

Replace the running configuration in partition **x** with the configuration in the system configuration files.

load config partitions all

Replace the running configuration in all partitions with the configuration in the system configuration files.

load config from-terminal

Replace the running configuration with what is entered from the terminal.

1. Type the initial command.
2. The system responds with a confirmation prompt, type Y to confirm.

Replace the running configuration? (y/n) y

3. Type in the replacement configuration entries.

```
net self-allow {
   defaults {
      ospf:any
      tcp:161
      tcp:22
      tcp:4353
      tcp:443
      tcp:53
      udp:1026
      udp:161
      udp:4353
      udp:520
      udp:53
   }
}
net stp-globals {
   config-name 00-01-D7-B5-67-00
}
sys management-ip 172.27.41.70/24 { }
sys management-route default {
   gateway 172.27.41.254
}
sys provision ltm {
   level nominal
}
....
```

ltm pool pool1 {
slow-ramp-time 200
}
.....
^D4. Use Ctrl+D to submit the changes or Ctrl+C to cancel the changes.

delete config file myfile

Delete **myfile** in default directory, **/var/local/scf/**.

list config file

Display files in default directory, **/var/local/scf/**.

Options

- **base**
  Indicates the base configuration. This option cannot be specified with the **binary**, **default**, **gtm-only**, and **user-only** options.
- **binary**
  Indicates binary configuration. This option may not be specified with any other options.
- **default**
  Indicates factory default configuration. This option cannot be specified with any other options.
- **file**
  Loads or saves a configuration from the specified file. For save, a file with a relative path is saved in the default directory, **/var/local/scf**. For load, in shell mode, the default directory, **/var/local/scf**, is used for a file with a relative path. In bash mode, for a file with a relative path, the current directory is searched first. If the file can't be found in the current directory, **/var/local/scf** is searched.
  This option can be used with **binary**, **default**, **from-terminal** and **partitions** options.
- **passphrase**
  Specifies a password to save or load an encrypted configuration file. This option can only be used with option **file**.
- **tar-file**
  Loads or saves disk files referred to by the configuration from the specified tar file. A file with a relative path is looked up, relative to the current directory.
- **files-folder**
  Loads disk files referred to by the configuration from the folder tree under the specified folder. Disk files by name are searched for recursively. When there is more than one file with the same name, the relative path of the file from the cache-path is used for selection.

- **from-terminal**
  Specifies that the configuration will be input from the terminal in the same format as the system configuration files in <B/config>. Use Ctrl+D to submit the changes and Ctrl+C to cancel the changes.
  This option cannot be specified with **default**, **file** and **partitions**.
- **gtm-only**
  Indicates the Global Traffic Manage (GTM) configuration. This option cannot be specified with the **base**, **exclude-gtm**, and **user-only** options.
- **exclude-gtm**
  Indicates the BIG-IP configuration, excluding GTMs. This is only valid with the **file** option. This option cannot be specified with the **base**, **gtm-only**, and **user-only** options.
- **merge**
  Loads the configuration from the specified file or from the terminal, which modifies the running configuration. If merging from the terminal, it requires Ctrl+D to complete the operation. This option is only valid with the **file** or **from-terminal** options.
- **partitions**
  Indicates the partitions in which configuration components reside. This option cannot be specified with the **default**, **file**, **from-terminal**, or **merge** options.
- **user-only**
  Indicates the configuration including user account information only. This option cannot be specified with the **base**, **default**, **exclude-gtm**, or **gtm-only** options.
- **time-stamp**
  Inserts a time-stamp in a file name. This is only valid with the **file** option.
- **verify**
  Validates the specified configuration from file(s) or from the terminal without changing the running configuration.
- **wait**
  Specifies that **tmsh** should wait for another instance of **tmsh** to finish saving the configuration before proceeding. If **wait** is not specified and another instance of **tmsh** is in the process of saving the configuration, the command exits **tmsh** immediately (because the other instance of **tmsh** is already saving the configuration).

See Also

load, *save*, *tmsh*

config-diff

Displays the differences between two specified single configuration files (SCFs).

Syntax

Display information using the **config-diff** component within the **sys** module with the syntax in the following section.

Display

```
show config-diff [file name] [file name]
```

Description

You can use the **config-diff** component to display the differences between two previously created SCF files.

Examples

show config-diff my.scf your.scf

Displays information about the differences between two specified files.

Options

- **file name**
  Specifies the name of an SCF file that you want to compare to another SCF file.

See Also

show, *tmsh*

connection

Sets idle timeout for, displays, and deletes active connections on the BIG-IP® system.

Syntax

Use the **connection** component within the **sys** module to manage connections using the following syntax.

Modify

```
modify connection
    idle-timeout [integer]
```

Display

```
show connection
  option:
    all-properties
    age [integer]
    cs-client-addr [IP address]
    cs-client-port [ [integer] | [service] ]
    cs-server-addr [IP address]
    cs-server-port [ [integer] | [service] ]
    (default | exa | gig | kil | meg | peta | raw | tera | yotta | zetta)
    protocol [name]
    save-to-file [ filename ]
    ss-client-addr [IP address]
    ss-client-port [ [integer] | [service] ]
    ss-server-addr [IP address]
    ss-server-port [ [integer] | [service] ]
    type [any | mirror | self]
```

Delete

```
delete connection
  option:
    age [integer]
    cs-client-addr [IP address]
    cs-client-port [ [integer] | [service] ]
    cs-server-addr [IP address]
    cs-server-port [ [integer] | [service] ]
    protocol [name]
    ss-client-addr [IP address]
    ss-client-port [ [integer] | [service] ]
    ss-server-addr [IP address]
    ss-server-port [ [integer] | [service] ]
    type [any | mirror | self]
```

Description

You can use the **connection** component to set the idle timeout for or delete active connections to the BIG-IP system based on a specified filter. Additionally, you can display information about the active connections to the system.

You can specify the <port> option using either a number or a service (80 or http).

Important

If you do not specify a port or service, the system deletes all connections that match just the IP address. If you do not specify an IP address, the system deletes all connections including mirrored connections.

Examples

show connection all-properties

Displays information about all active connections to the system.

modify connection idle-timeout 300

Changes the amount of idle time before a connection is disconnected to five minutes (300 seconds).

Options

- **age**
  Specifies, in seconds, the age of the active connections that you want to display or delete.
- **cs-client-addr**
  Specifies the client-side remote IP address of the active connections that you want to display or delete.
- **cs-client-port**
  Specifies the clientside remote port of the active connections that you want to display or delete.
- **cs-server-addr**
  Specifies the clientside local IP address of the active connections that you want to display or delete.
- **cs-server-port**
  Specifes the clientside local port of the active connections that you want to display or delete.
- **idle-timeout**
  Specifies the interval, in seconds, that a connection can remain idle before the system closes the connection.
- **protocol**
  Specifies the protocol of the active connections that you want to display or delete.

- **save-to-file**
  Specifies the file which connection information can be save to. With this option, it can write a file larger than 2GB.
- **ss-client-addr**
  Specifes the serverside local IP address of the active connections that you want to display or delete.
- **ss-client-port**
  Specifes the serverside local port of the active connections that you want to display or delete.
- **ss-server-addr**
  Specifes the serverside remote IP address of the active connections that you want to display or delete.
- **ss-server-port**
  Specifes the serverside remote port of the active connections that you want to display or delete.
- **type**
  Specifes the type of active connections that you want to display or delete. The possible values are:
  - **any**
    Specifies all active connections.
  - **mirror**
    Specifies only mirrored connections.
  - **self**
    Specifies the connection with which you are accessing the system.

See Also

delete, *modify*, *show*, *tmsh*

console

Configures the serial console for the BIG-IP® system.

Syntax

Configure the **console** component within the **sys** module using the syntax in the following section.

Modify

```
modify console
    baud-rate [integer]
```

Display

```
show console
```

Description

You can use the **console** component to configure the serial console on the BIG-IP system.

Options

- **baud-rate**
  Specifies the baud rate for the serial console. Select from the following options:
  - **9600**
  - **19200** (default)
  - **57600**
  - **115200**

For information about the options that you can use with the command **show**, see **help show**.

See Also

modify, *show*, *tmsh*

cpu

Displays statistics about the Traffic Management Microkernel (TMM) service, specifically, CPU cycles.

Syntax

Display statistics for the **cpu** component within the **sys** module using the syntax in the following section.

Display

```
show cpu
    (default | exa | gig | kil | meg | peta | raw | tera | yotta | zetta)
    global
```

Description

You can use the **cpu** component to display the CPU cycles for the system. You can also specify the unit value in which the system displays statistics.

Examples

show cpu

Displays TMM processer statistics in the system default units.

show cpu raw

Displays raw TMM processer statistics.

See Also

show, *tmsh*

daemon-ha

Configures high availability for a BIG-IP® system.

Syntax

Configure the **daemon-ha** component within the **sys** module using the syntax in the following sections.

Modify

```
modify daemon-ha [name]
    heartbeat [enabled | disabled]
    heartbeat-action [go-offline | go-offline-downlinks-restart |
      go-offline-restart | reboot | restart | restart-all]
    running [enabled | disabled]
edit daemon-ha [ [ [name] | [glob] | [regex] ] ... ]
    all-properties
    non-default-properties
```

Display

```
list daemon-ha
list daemon-ha [ [ [name] | [glob] | [regex] ] ... ]
show running-config daemon-ha
show running-config daemon-ha [ [ [name] | [glob] | [regex] ] ... ]
    all-properties
    non-default-properties
    not-running-action
    one-line
    running-timeout
```

Description

You can use the **daemon-ha** component to configure the daemons on the system that handle high availability for the BIG-IP system.

Examples

modify daemon-ha bigd running disabled

Disables the **bigd** daemon.

list daemon-ha bigd running-timeout

Displays the running timeout of the **bigd** daemon.

Options

- **glob**
  Displays the items that match the **glob** expression. See **help glob** for a description of **glob** expression syntax.
- **heartbeat**
  Specifies whether heartbeat monitoring is enabled for the specified daemon. If monitoring is enabled and the daemon does not maintain its heartbeat the action specified by the value of the **heartbeat-action** option is taken.
  The default value is **enabled** for all daemons, except the **named** daemon, which is **disabled** by default.
- **heartbeat-action**
  Specifies the action the system takes if the specified daemon does not maintain its heartbeat.
  The default value is dependent on the specified daemon, the most common default value is **restart**.
- **name**
  Specifies a unique name for the component. This option is required for the command **modify**.
- **not-running-action**
  Specifies the action that the system takes if the daemon is not running. This option is read-only.
  The default value is dependent on the specified daemon, the most common default value is **go-offline-downlinks**.
- **regex**
  Displays the items that match the regular expression. The regular expression must be preceded by an at sign (@[regular expression]) to indicate that the identifier is a regular expression. See **help regex** for a description of regular expression syntax.
- **running**
  Specifies whether the **running-timeout** and **non-running-action** options are **enabled**. The default value is dependent on the specified daemon, the most common default value is **enabled**.

◆ Note

This feature is implemented only for the daemons: ***tmm****,* ***mcpd****,* ***bcm56xxd****,* ***bigd****,* ***gtmd****,* ***clusterd****,* ***tmrouted****,* ***bd****,* ***datasyncd*** *and* ***tmrouted****.*

- **running-timeout**
  Specifies the amount of time (in seconds) that must elapse before the specified daemon is considered to be not running. This option is read-only.
  The default value is dependent on the specified daemon.

See Also

edit, glob, *list*, *modify*, regex, *show*, *tmsh*

datastor

Configures the data storage used for optimization.

Syntax

Configure the **datastor** component within the **sys** module using the syntax in the following sections.

Modify

```
modify datastor
    dedup-cache-weight [integer]
    description [string]
    disk [disabled | enabled]
    high-water-mark [integer]
    low-water-mark [integer]
    web-cache-weight [integer]
```

Display

```
list datastor
show running-config datastor
    all-properties
    cache-size
    non-default-properties
    one-line
    store-size
```

Description

You can use the **datastor** component to configure disk I/O operations and optimized page cache for frequently accessed sectors. Note that symmetric data deduplication is one consumer of this storage space.

Examples

list datastor all-properties

Displays the data storage settings.

modify datastor disk disabled

Disables data storage on the disk.

Options

- **cache-size**
  Displays the size of the data storage in megabytes (MB).

- **dedup-cache-weight**
  Specifies the relative weight of the dedup cache for the Acceleration Manager module. The default value is **10**.
- **description**
  User defined description.
- **disk**
  Enables or disables the use of the disk (in addition to memory) for data storage.
  If you enable or disable data storage on the disk, you must then restart the **datastor** service from the command line using the command sequence **bigstart restart datastor**.
- **high-water-mark**
  Specifies the percentage of full cache above which pruning starts. The valid range is **60** - **100** percent. The default value is **92**.
- **low-water-mark**
  Specifies the percentage of full cache below which pruning stops. The valid range is **10** - **90** percent. The default value is **80**.
- **store-size**
  Displays the amount of space for each disk path specified.
- **web-cache-weight**
  Specifies the relative weight of the web cache for the Acceleration Manager module. The default value is **10**.

See Also

deduplication, *list*, *modify*, *show*, *tmsh*

db

Displays or modifies bigdb database entries.

Syntax

Configure the **db** component within the **sys** module using the syntax in the following sections.

Modify

```
modify db [name] value [database variable value]
modify db [name] reset-to-default
```

Display

```
list db
list db [ [ [name] | [glob] | [regex] ] ...]
    all-properties
    default-value
    non-default-properties
    one-line
    value
    value-range
show running-config db
show running-config db [ [ [name] | [glob] | [regex] ] ...]
    all-properties
```

Description

You can use the **db** component to modify and retrieve the data that is stored in the bigdb configuration database.

Important

*After you change a **bigdb** database variable using the **db** component, you must run the command sequence **save config**. If you do not, the next time that you run the command sequence **load [config base | config]**, the value of the **bigdb** database variable may be reset to the value in the stored configuration.*

Note that **tmsh** only displays bigdb database entries when you explicitly request them.

Examples

modify db Connection.SynCookies.Threshold value 16384

Sets the database entry, **SYN Check™ Activation Threshold**, to the given value.

modify db Connection.SynCookies.Threshold reset-to-default

Sets the database entry, **SYN Check™ Activation Threshold**, back to the default value.

list log.mcpd.level

Displays the properties of the database entry **log.mcpd.level**:

Options

- **default-value**
  Displays the system-supplied default value of the database entry.
- **glob**
  Displays the items that match the **glob** expression. See **help glob** for a description of **glob** expression syntax.
- **name**
  Specifies the unique name of the database variable. This option is required for the command **modify**.
- **regex**
  Displays the items that match the regular expression. The regular expression must be preceded by an at sign (@[regular expression]) to indicate that the identifier is a regular expression. See **help regex** for a description of regular expression syntax.
- **reset-to-default**
  Resets the database variable back to its default value.
- **value**
  Specifies the value to which you want to set the specified database entry.
- **value-range**
  Displays the type of data that you can use with the value option. The options are:
  - **integer**
  - **IP address**
  - **list of valid values**
  - **management IP address**
  - **string**
  - **unsigned integer**

See Also

glob, *list*, *modify*, regex, *show*, *tmsh*

default-config

Loads the default configuration of the BIG-IP® system stored in the configuration files to the running configuration of the system.

Syntax

Configure the **default-config** component within the **sys** module using the following syntax.

Modify

```
load default-config
```

Description

You can use the **default-config** component to load the default system configuration to the running configuration. This results in the user-defined configuration being removed from the running configuration.

Examples

load default-config

Loads the default configuration stored on the system to the running configuration of the system.

See Also

load, *tmsh*

dns

Configures the Domain Name System (DNS) for the BIG-IP® system.

Syntax

Modify the **dns** component within the **sys** module using the syntax shown in the following sections.

Modify

```
modify dns
    description [string]
    include [string]
    name-servers [add | delete | replace-all-with] {
      [IP address] ...
    }
    name-servers none
    search [add | delete | replace-all-with] {
      [domain] ...
    }
    search none
edit dns
    all-properties
    non-default-properties
```

Display

```
list dns
list dns [option]
show running-config dns
show running-config dns [option]
    all-properties
    non-default-properties
    one-line
```

Description

You can use the **dns** component to manage configurations by server grouping, in this case, DNS servers.

Examples

- **modify dns name-servers add { 192.168.10.20 192.168.10.22 }**
  Adds DNS name servers with the IP addresses, **192.168.10.20** and **192.168.10.22**, to the BIG-IP system.

- **modify dns search add { siterequest.com store.siterequest.com london.siterequest.com }**
  Adds the host names, **siterequest.com**, **store.siterequest.com**, and **london.siterequest.com**, to the DNS search configuration for the BIG-IP system.

Note

When DNS searches for the host, siterequest, which is not a fully qualified domain name, it uses the IP address of the first match, in this case, siterequest.com.

- **show running-configuration dns**
  Displays the running configuration of the **dns** component.

Options

- **description**
  User defined description.
- **include**

WARNING

Do not use this option without assistance from the F5 Technical Support team. *The system does not validate the commands issued using the include option. If you use this option incorrectly, you put the functionality of the system at risk.*

- **name-servers**
  Configures a group of DNS name servers for the BIG-IP system.
- **search**
  Configures a list of domain names in a specific order. DNS uses that order when searching for host names that are not fully qualified. You can use this option to delete domain names in the list.

See Also

edit, *list*, *modify*, *tmsh*

failover

Configures failover for a BIG-IP® unit in a redundant system configuration.

Syntax

Change the **failover** state within the **sys** module using the syntax in the following section.

Modify

```
run failover
     device [string]
     no-persist
     offline
     online
     persist
     standby
     traffic-group [[string] | default | non-default | none]
```

Display

```
show failover
   cable
```

Description

Failover is the process where a standby unit in a redundant system configuration takes over when a software or hardware failure is detected on the active unit.

Examples

run failover standby

Causes the active unit or cluster to go into the standby state forcing the other unit or cluster in the redundant system configuration to become active.

run failover offline

Causes the active unit or cluster to go into the Forced Offline state.

run failover online

Changes the status of a unit or cluster from Forced Offline to either Active or Standby, depending upon the status of the other unit or cluster in a redundant system configuration.

show failover

Displays the failover state of the BIG-IP system (active, standby, offline) and how long it has been in that state.

run failover standby device my_bigip

Specifies that the my_bigip device should become the active device for all traffic groups.

run failover standby traffic-group traffic_grp01

Specifies that the traffic group named **traffic_grp01** should fail over to the Standby state. The traffic group will then become Active on another device.

run sys failover offline no-persist

Changes the status of a unit to Forced Offline and indicates that the change will not be persisted after a system restart.

run sys failover offline persist

Changes the status of a unit to Forced Offline and indicates that the change will be persisted after a system restart.

Options

Use these options to control failover of the system:

- **device**
  Specifies the device that should next become the active device for the specified traffic group or all traffic groups (if a traffic group is not specified). This option may only be specified with the standby option.
- **no-persist**
  Does not persist the change in status of a unit. The option is valid only with the **offline** state.
- **offline**
  Changes the status of a unit or cluster to Forced Offline. If **persist** or **no-persist** options are not specified, the default action is to persist the offline status of the unit between system restarts.
- **online**
  Changes the status of a unit or cluster from Forced Offline to either Active or Standby, depending upon the status of the other unit or cluster in a redundant system configuration.
- **persist**
  Persists the change in status of a unit. The option is valid only with the **offline** state.
- **standby**
  Specifies that the active unit or cluster fails over to a Standby state, causing the standby unit or cluster to become Active.
- **traffic-group**
  Specifies the traffic-group that should fail over to the Standby state, the traffic-group will become Active on another device. This option may only be specified with the standby option.

Use this option to display the failover cable status of the system:

- **cable**
  Displays the status that the failover daemon detects on the serial cable from its failover peer. It also shows what the failover peer detects on the serial cable. An active BIG-IP system will see a zero from its failover peer. A standby BIG-IP system will see a one from its failover peer.

See Also

run, *tmsh*

feature-module

Enables or disables a feature module on the BIG-IP® system.

Syntax

Configure the **feature-module** component within the **sys** module using the syntax in the following sections.

Modify

```
modify feature-module
modify feature-module [ [all] | [cgnat] ]
    enabled | disabled
edit feature-module
  [ [ [cgnat] | [glob] | [regex] ] ... ]
    all-properties
    non-default-properties
```

Display

```
list feature-module
list feature-module
  [ [ [cgnat] | [glob] | [regex] ] ... ]
    all-properties
    non-default-properties
    one-line
```

Description

You can use the **feature-module** component to modify the availability of any licensed feature modules on your system.

Examples

- **modify feature-module cgnat enabled**
  Enables the BIG-IP Carrier Grade NAT module.
- **modify feature-module cgnat disabled**
  Disables the BIG-IP Carrier Grade NAT module.
- **list feature-module**
  Displays the current feature module of the system.

Options

- **all**
  Specifies that you are enabling or disabling all of the available modules.

- **cgnat**
  Specifies that you are enabling or disabling the BIG-IP Carrier Grade NAT module.
- **glob**
  Displays the items that match the **glob** expression. See **help glob** for a description of **glob** expression syntax.
- **regex**
  Displays the items that match the regular expression. The regular expression must be preceded by an at sign (@[regular expression]) to indicate that the identifier is a regular expression. See **help regex** for a description of regular expression syntax.

See Also

edit, glob, *list*, *modify*, regex, *show*, *tmsh*, *provision*

fix-connection

Displays FIX connection statistics.

Syntax

Display

```
show fix-connection
    (default | exa | gig | kil | meg | peta | raw | tera | yotta | zetta)
   all-properties
   save-to-file
```

Description

You can use the **fix-connection** component to display statistics about FIX connections.

Examples

show fix-connection

Displays FIX connection statistics in the system default units.

Options

For information about the options that you can use with the command **show**, see **help show**.

folder

Configure folders (directory structure) on the BIG-IP® system.

Syntax

Configure the **folder** component within the **sys** module using the syntax in the following sections.

Create/Modify

```
create folder [name]
modify folder [name]
    app-service [[string] | none]
    description [string]
    device-group [[string] | default | non-default | none]
    no-ref-check [false | true]
    traffic-group [[string] | default | non-default | none]
```

Display

```
list folder
list folder [ [name] | [glob] | [regex] | [recursive] ]
```

Delete

```
delete folder [name]
```

Description

The folder system enables users to create logical containers for the purpose of granular control of synchronization to other devices in a device group.

The folder system is hierarchical, with folders and sub-folders, in a parent-to-child relationship. The highest level folder in the system is called **root**. For every administrative partition on the BIG-IP system, there is a top-level folder. Top-level folders always have root as the parent. Users can create sub-folders to any folder in the system.

Examples

create sys folder sub-folder1 device-group dg1 traffic-group none

Creates a new sub-folder to the current working folder called **sub-folder1**, associates the folder with a device-group called **dg1**, and sets the traffic-group to no association.

modify sys folder /Common/sub-folder1/subfolder2 description "store pools for the B2 server configuration"

Changes the description property of the folder indicated by its full name.

Options

- **app-service**
  Specifies the name of the application service to which the object belongs. The default value is **none**. **Note:** If the **strict-updates** option is **enabled** on the application service that owns the object, you cannot modify or delete the object. Only the application service can modify or delete the object.
- **description**
  User defined description.
- **device-group**
  Adds this folder and all configuration items in this folder to a device group for device failover or config-sync purposes. The options are:
  - **default**
    Indicates that this folder should use the device group setting of its parent folder. If the parent folder's associated device group is changed, this folder's device group will change as well.
  - **non-default**
    Disassociates this folder from its parent folder's device group setting. This folder's device group field can then be set independently of the parent folder's field.
- **hidden**
  Folders may be hidden by setting this property to **true**. The **-hidden** command-line option will allow you to view hidden folders, but is not required to use or modify a folder. The **-hidden** command-line option only affects output from the list command and the results of tab completing a configuration item. If set to **false**, the folder will always be visible as long as the user has the appropriate permissions.
- **inherited-devicegroup**
  Specifies, when set to **true**, that this folder uses the device group setting of its parent folder. If the parent folder's associated device group is changed then this folder's device group will change as well. This field is read-only.
- **inherited-traffic-group**
  Specifies, when set to **true**, that this folder uses the traffic group setting of its parent folder. If the parent folder's associated traffic group is changed then this folder's traffic group will change as well. This field is read-only.
- **no-ref-check**
  Specifies whether strict device group reference validation is performed on configuration items in the folder. The options are:
  - **false**
    Requires configuration items in the folder to sync to a super-set of the devices that are associated with any configuration that refers to configuration items in the folder. This is the default value.

- **true**
  Disables this check. It is then assumed that any dependent configuration items contained in the folder will be created locally on the other devices.

◆ **traffic-group**
Adds this folder and its configuration items to an existing traffic group. The values **default** and **non-default** work as they do for the **device-group** option.

See Also

create, *delete*, glob, *list*, *modify*, regex, *tmsh*

geoip

Loads the GeoIP data files.

Syntax

Use the **geoip** component within the **gtm** module to load the GeoIP data files using the syntax in the following sections.

Loading

```
load geoip
```

Description

The BIG-IP system ships with three default database files that are stored in the **/usr/share/GeoIP/** directory. The three files are: **F5GeoIP.dat**, **F5GeoIPISP.dat**, and **F5GeoIPv6.dat**.

You can download and install updated GeoIP database files using the procedure available from the F5 download site. The installation places the updated database files in the **share/GeoIP** directory.

When you run the **load geoip** command sequence, the system loads the GeoIP files from disk into the running configuration. If you have downloaded and installed updated database files, those files are loaded from the **/shared/GeoIP** directory. Otherwise, the default database files are loaded from the **/usr/share/GeoIP/** directory. Note that if both directories contain the same files, the files in **shared/GeoIP** are loaded.

Examples

load geoip

Loads the GeoIP files from disk into the running configuration.

See Also

load, *tmsh*

global-settings

Configures the global system settings for a BIG-IP® system.

Syntax

Configure the **global-settings** component within the **sys** module using the syntax in the following sections.

Modify

```
modify global-settings
    aws-access-key [string]
    aws-secret-key [string]
    aws-api-max-concurrency [integer]
    console-inactivity-timeout [integer]
    custom-addr [IP address]
    description [string]
    failsafe-action [go-offline | reboot | resetart-all |
                     go-offline-restart-tm | failover-restart-tm]
    file-local-path-prefix [local path prefix]
    gui-security-banner [disabled | enabled]
    gui-security-banner-text [string]
    gui-setup [disabled | enabled]
    host-addr-mode [custom | management | state-mirror]
    hostname [string]
    hosts-allow-include [string]
    lcd-display [disabled | enabled]
    net-reboot [disabled | enabled]
    password-prompt [string]
    mgmt-dhcp [disabled | enabled]
    quiet-boot [disabled | enabled]
    remote-host [add | delete | replace-all-with] {
      [name]... {
          addr [IP address]
          hostname [string]
      }
    }
    remote-host none
    username-prompt [string]
edit global-settings
    all-properties
    non-default-properties
```

Display

```
list global-settings
list global-settings [option]
show running-config global-settings
show running-config global-settings [option]
    all-properties
    non-default-properties
    one-line
```

Description

You can use the **global-settings** component to set up the BIG-IP system.

Examples

modify system remote-host add { bigip151 {addr 172.27.226.151 hostname bigip151.saxon.net} }

Sets up a remote host named **bigip151** with an IP address of **172.27.226.151** and a hostname of **bigip151.saxon.net**.

list global-settings all-properties

Displays all of the properties of the global system settings.

Options

- **aws-access-key**
  Amazon Web Services (AWS) supplied access key needed to make secure requests to AWS. The default value is **none**.
- **aws-secret-key**
  Amazon Web Services (AWS) supplied secret key needed to make secure requests to AWS. The default value is **none**.
- **aws-api-max-concurrency**
  Maximum concurrent connections allowed while making Amazon Web Service (AWS) api calls. The default value is **1**.
- **console-inactivity-timeout**
  Specifies the number of seconds of inactivity before the system logs off a user that is logged on. The default value is **0** (zero), which means that no timeout is set. The valid range is **0** - **2147483647**.
- **custom-addr**
  Specifies an IP address for the system. The default value is **::**. The **host-addr-mode** option must be set to **custom** in order for this setting to take effect.
- **description**
  Specifies a user defined description. The default value is no description.
- **failsafe-action**
  Specifies the action that the system takes when the switch board fails. The default value is **go-offline-restart-tm**.
  - **failover-restart-tm**
    Specifies that when the switch board fails the system restarts the traffic management system and fails over to the other unit in a redundant pair.
  - **go-offline**
    Specifies that when the switch board fails the system goes offline.

- **go-offline-restart-tm**
  Specifies that when the switch board fails the system goes offline and restarts the traffic management system.
- **reboot**
  Specifies that after the active cluster fails over to its peer, it reboots while the peer processes the traffic.
- **restart-all**
  Specifies that when the switch board fails the system restarts all system services.

◆ **file-local-path-prefix**
Specifies a list of folder prefixes that can be applied for file objects. This is a space separated list of folder prefixes, contained in curly braces. Example: "{file:///shared/}" or "{file:///fileobjectfolder/} {/shared/}". By default the folders are "/shared/" and "/tmp/", represented as "{/shared/} {/tmp/}".

◆ **gui-security-banner**
Specifies whether the system presents on the login screen the text you specify in the **gui-security-banner-text** option. If you disable this option, the system presents an empty frame in the right portion of the login screen. The default value is **enabled**.

◆ **gui-security-banner-text**
Specifies the text to present on the login screen when the **gui-security-banner** option is enabled. The default value is **Welcome to the BIG-IP Configuration Utility**.

◆ Note

*To enter a carriage return in the text type **Ctrl-V** followed by **Ctrl-J**. Additionally, you must escape special characters, such as a question mark(?), with a back slash.*

◆ **gui-setup**
Enables or disables the Setup utility in the browser-based Configuration utility. The default value is **enabled**.

◆ Note

*When you configure a system using **tmsh**, disable this option. Disabling this option allows the system administrators to use the browser-based Configuration utility without having to run the Setup utility.*

◆ **host-addr-mode**
Specifies the type of host address you want to assign to the system. The default value is **management**. The options are:

- **custom**
  Use this value to specify a custom IP address for the system using the **custom-addr** option.
- **management**
  Indicates that the host address is the management port of the system.

- **state-mirror**
  Use this value when the host address of the system is shared by the other system in a redundant pair. In case of system failure, the traffic to the other system is routed to this system.

- **hostname**
  Specifies a local name for the system. The default value is **bigip1**.
- **hosts-allow-include**

WARNING

*Do not use this parameter without assistance from the F5 Technical Support team. The system does not validate the commands issued when you use the **hosts-allow-include** option. If you use this option incorrectly, you put the functionality of the system at risk.*

- **lcd-display**
  Enables or disables the LCD display on the front of the system. The default value is **enabled**.
- **net-reboot**
  Enables or disables the network reboot feature. The default value is **disabled**.
  If you enable this feature and then reboot the system, the system boots from an ISO image on the network, rather than from an internal media drive. Use this option only when you want to install software on the system, for example, for an upgrade or a re-installation.

Note

*An **enabled** value reverts to **disabled** after you reboot the system a second time.*

- **password-prompt**
  Specifies the text to present above the password field on the system's login screen.
- **mgmt-dhcp**
  Specifies whether the system uses DHCP client for acquiring the management interface IP address. If this option is enabled, manually specified IP addresses for the management interface may be overwritten if the network also contains a DHCP server. If this option is disabled, no DHCP server will be applied to the management interface, however any previously acquired address will still be used. The default value is **enabled** for VE and **disabled** for all other platforms. When this option is enabled, manual changes like create/delete on management-ip will not be allowed.
- **quiet-boot**
  Enables or disables the quiet boot feature. The default value is **enabled**. When **enabled**, the system suppresses informational text on the console during the boot cycle.

- **remote-host**
  Configures a remote host in the **/etc/hosts** file. The default value is **none**. You must enter both an IP address and a fully qualified domain name (FQDN) or alias for each host that you want to add to the file.
- **username-prompt**
  Specifies the text to present above the user name field on the system's login screen.

See Also

edit, *list*, *modify*, *show*, *tmsh*

ha-group

Configures the high availability (HA) scoring mechanism for a unit in a traffic group of BIG-IP® systems.

Syntax

Configure the **ha-group** component within the **sys** module using the following syntax.

Create/Modify

```
create ha-group [name]
modify ha-group [name]
   active-bonus [integer]
   app-service [[string] | none]
   clusters none
   clusters [add | delete | modify | replace-all-with] {
     [name] {
       app-service [[string] | none]
       attribute percent-up-members
       threshold [integer]
       weight [integer]
     }
   }
   description [string]
   [disabled | enabled]
   pools none
   pools [add | delete | modify | replace-all-with] {
     [name] {
       app-service [[string] | none]
       attribute percent-up-members
       threshold [integer]
       weight [integer]
     }
   }
   trunks none
   trunks [add | delete | modify | replace-all-with] {
     [name] {
       app-service [[string] | none]
       attribute percent-up-members
       threshold [integer]
       weight [integer]
     }
   }
```

Display

```
list ha-group
list ha-group [name]
    all
    all-properties
    current-module
    one-line
```

Delete

```
delete ha-group [name]
```

Description

You can use the **ha-group** component to configure a high availability (HA) group that determines the HA scoring mechanism for a unit in a traffic group. This mechanism compares the relative health of the two or more units in the traffic group and the system with the highest score becomes the active unit. **Note** Use the attribute ha-group of the traffic group to make the association.

Examples

create ha-group group1 pools add { ftp_pool { attribute percent-up-members weight 70 } }

Creates a HA group, named **group1**, that includes the pool named **ftp_pool**, and uses the attribute **percent-up-members** and a weight of **70** to determine the HA score for a unit in a traffic group.

list ha-group group1

Displays the configuration of the HA group, **group1**.

Options

- **active-bonus**
  Specifies a number to add to the unit's HA score when the unit is **active**. This option ensures that the state of a unit is dependent upon the history of its state. The default value is **10** (ten). The range is **0** - **100**.
- **app-service**
  Specifies the name of the application service to which the object belongs. The default value is **none**. **Note:** If the **strict-updates** option is **enabled** on the application service that owns the object, you cannot modify or delete the object. Only the application service can modify or delete the object.
- **attribute**
  Specifies an attribute of the component that you want to use for the HA scoring mechanism. **Percent-up-members** is the only available attribute for HA scoring for the **clusters**, **pools**, and **trunks** options.
- **clusters**
  Specifies the clusters that you want to configure for the HA group. You can only configure a cluster on a chassis.
- **description**
  User defined description.

- **[disabled | enabled]**
  Enables or disables the HA group in the HA table. The default value is **enabled**.
- **name**
  Specifies the name of the component that you want to configure. This option is required when you create, modify, or delete a HA group. This option is also required when you configure clusters, pools, or trunks for the HA group.
- **pools**
  Specifies the pools that you want to configure for the HA group.
- **threshold**
  Specifies the minimum number of **up** interfaces in a trunk, **up** pool members in a pool, or **up** cluster members in a cluster below which the specified component does not contribute to the HA score for the unit. The default value is **0** (zero), which indicates this option is disabled. The value may not exceed the number of members of the trunk, pool, or cluster.
- **trunks**
  Specifies the trunks that you want to configure for the HA group.
- **weight**
  The value of this option is multiplied by the percent of **up** cluster, pool, or trunk members, and is added to the HA score. The default value is **10**. The range is **10** - **100**.

See Also

create, *delete*, *list*, *modify*, *tmsh*

ha-status

Displays information about the high availability (HA) status of a unit in a redundant pair.

Syntax

Display information about the **ha-status** component within the **sys** module using the following syntax.

Display

```
show ha-status
    all-properties
    (default | exa | gig | kil | meg | peta | raw | tera | yotta | zetta)
    field-fmt
```

Description

You can use the **ha-status** component to display information about the high availability status of a unit in a redundant pair.

Examples

show ha-status

Display information about the HA status of the unit.

Options

For information about the options that you can use with the command **show**, see **help show**.

See Also

show, *tmsh*

hardware

Displays the BIG-IP® system hardware.

Syntax

Display statistics for the **hardware** component within the **sys** module using the syntax in the following section.

Display

```
show hardware
```

Description

You can use the **hardware** component to display information about the hardware.

Examples

show hardware

Displays hardware information for the system.

Options

For information about the options that you can use with the command **show**, see **help show**.

See Also

show, *tmsh*

host-info

Displays statistics about the host.

Syntax

Configure the **host-info** component within the **sys** module using the syntax in the following sections.

Display

```
show host-info
    (default | exa | gig | kil | meg | peta | raw | tera | yotta | zetta)
    global
```

Description

You can use the **host-info** component to display statistics about the host, including CPU count, active CPU count, processor mode, memory usage, and more.

Examples

show host-info

Displays host statistics in the system default units.

show host-info raw

Displays raw host statistics.

Options

For information about the options that you can use with the command **show**, see **help show**.

See Also

show, *tmsh*

httpd

Configures the HTTP daemon for the BIG-IP® system.

Syntax

Configure the **httpd** component within the **sys** module using the following syntax.

Create/Modify

```
modify httpd
    allow [add | delete | none |replace-all-with] {
      hostname or IP address ...
    }
    auth-name [string]
    auth-pam-dashboard-timeout [off | on]
    auth-pam-idle-timeout [integer]
    auth-pam-validate-ip [off | on]
    description [string]
    fastcgi-timeout [integer]
    hostname-lookup [double | off | on]
    include [string]
    log-level [alert | crit | debug | emerg | error | info | notice | warn]
    redirect-http-to-https [disabled | enabled]
    request-header-max-timeout [integer]
    request-header-min-rate [integer]
    request-header-timeout [integer]
    request-body-max-timeout [integer]
    request-body-min-rate [integer]
    request-body-timeout [integer]
    ssl-ca-cert-file [string]
    ssl-certchainfile [string]
    ssl-certfile [string]
    ssl-certkeyfile [string]
    ssl-ciphersuite [string]
    ssl-include [string]
    ssl-protocol [string]
    ssl-verify-client [no | require | optional | optional-no-ca]
    ssl-verify-depth [integer]
    ssl-ocsp-enable [on | off]
    ssl-ocsp-default-responder [string]
    ssl-ocsp-override-responder [on | off]
    ssl-ocsp-responder-timeout [integer]
    ssl-ocsp-response-max-age [integer]
    ssl-ocsp-response-time-skew [integer]
edit httpd
    all-properties
    non-default-properties
```

Display

```
list httpd
list httpd [option name]
show running-config httpd
show running-config httpd [option name]
```

```
all-properties
non-default-properties
one-line
```

Description

You can use the **httpd** component to configure the HTTP daemon for the system.

Important

*F5 Networks recommends that users of the Configuration utility exit the utility before changes are made to the system using the **httpd** component. This is because making changes to the system using this component causes a restart of the **httpd** daemon. Additionally, restarting the **httpd** daemon creates the necessity for a restart of the Configuration utility.*

Examples

modify httpd { ssl-certfile [string] ssl-certkeyfile [string] }

Changes the SSL certificate and the SSL key. Note that when you change the SSL key, you must also change the SSL certificate.

modify httpd auth-pam-idle-timeout 43200

Sets the PAM idle timeout to half a day (in seconds).

modify httpd allow replace-all-with {172.27.0.0/255.255.0.0}

Replaces the existing list of hosts that can connect to the **httpd** daemon with the hosts in the range, **172.27.0.0/255.255.0.0**.

Options

- **allow**
  Configures IP addresses and hostnames for the HTTP clients from which the **httpd** daemon accepts requests. The default value is **All**.

WARNING

*Using the value **none** resets the **httpd** daemon to allow all HTTP clients access to the system; therefore, F5 Networks recommends that you do not use the value **none**.*

- **auth-name**
  Specifies the name for the authentication realm. The default value is **BIG-IP**.
- **auth-pam-dashboard-timeout**
  Specifies whether idle timeout while viewing the dashboard is enforced or not. The default value is **off**.

- **auth-pam-idle-timeout**
  Specifies the number of seconds of inactivity that can elapse before the GUI session is automatically logged out. The default value is **1200** seconds.
- **auth-pam-validate-ip**
  Specifies whether the check for consistent inbound IP for the entire web session is enforced or not. The default value is **on**.
- **description**
  User defined description.
- **fast-cgitimeout**
  Specifies, in seconds, the timeout for FastCGI. The default value is **300** seconds.
- **hostname-lookup**
  The default value is **off**.
- **include**
  The default value is **none**.

WARNING

*Do not use this option without assistance from the F5 Technical Support team. The system does not validate the commands issued using this option. If you use the **include** option incorrectly, you put the functionality of the system at risk.*

- **log-level**
  Specifies the minimum httpd message level to include in the system log. The default value is **warn**.
- **redirect-http-to-https**
  Specifies whether the system should redirect HTTP requests targeted at the configuration utility to HTTPS. The default value is **disabled**.
- **request-header-max-timeout**
  Specifies, in seconds, the maximum time allowed to receive all of the request headers, if the **request-header-min-rate** option is used, in which case the timeout is extended as more data arrives. Ignored if **request-header-min-rate** is not used. A value of 0 means no limit. The default value is **40**.
- **request-header-min-rate**
  Specifies, in bytes per second, the minimum average rate at which the request headers must be received. A value of 0 means no limit. The default value is **500**.
- **request-header-timeout**
  Specifies, in seconds, the time allowed to receive all of the request headers. A value of 0 means no limit. If you use the

request-header-min-rate option, this represents the initial value for the timeout, which will be extended as more data arrives. The default value is **20**.

WARNING

This includes the time needed to complete the initial SSL handshake. If the user's browser is configured to query certificate revocation lists and the CRL server is not reachable, the initial SSL handshake may take a significant time until the browser gives up waiting for the CRL.

- **request-body-max-timeout**
  Specifies, in seconds, the maximum time allowed to receive all of the request body, if the **request-body-min-rate** option is used, in which case the timeout is extended as more data arrives. Ignored if **request-body-min-rate** is not used. A value of 0 means no limit. The default value is **0**.
- **request-body-min-rate**
  Specifies, in bytes per second, the minimum average rate at which the request body must be received. A value of 0 means no limit. The default value is **500**.
- **request-body-timeout**
  Specifies, in seconds, the time allowed for reading all of the request body. This includes the time needed to do any SSL renegotiation. A value of 0 means no limit. If you use the **request-body-min-rate** option, this represents the initial value for the timeout, which will be extended as more data arrives. The default value is **60**.
- **ssl-ca-cert-file**
  Specifies the name of the file that contains the SSL Certificate Authority (CA) certificate file. The default value is **none**.
- **ssl-certchainfile**
  Specifies the name of the file that contains the SSL certificate chain. The default value is **none**.
- **ssl-certfile**
  Specifies the name of the file that contains the SSL certificate. The default value is **/etc/httpd/conf/ssl.crt/server.crt**.
  Note that the path to the file must start with either **/etc/httpd/conf/ssl.crt/** or **/config/httpd/conf/ssl.crt/**, unless the path is a relative path. If the path is a relative path, then it must start with **conf/ssl.crt/**.
- **ssl-certkeyfile**
  Specifies the name of the file that contains the SSL certificate key. The default value is **/etc/httpd/conf/ssl.key/server.key**.
  Note that the path to the file must start with either **/etc/httpd/conf/ssl.key/** or **/config/httpd/conf/ssl.key/**, unless the path is a relative path. If the path is a relative path, then it must start with **conf/ssl.key/**.
  When you change the key file, you must also change the certificate file. For example, use the following command sequence to change the key:
  modify httpd { ssl-certfile [string] ssl-certkeyfile [string] }

- **ssl-ciphersuite**
  Specifies the ciphers that the system uses. The default value is **"ALL:!ADH:!EXPORT:!eNULL:!MD5:!DES:RC4+RSA:+HIGH:+MEDIUM:+LOW:+SSLv2"**
- **ssl-include**
  The default value is **none**.

WARNING

*Do not use this option without assistance from the F5 Technical Support team. The system does not validate the commands issued using this option. If you use the **ssl-include** option incorrectly, you put the functionality of the system at risk.*

- **ssl-protocol**
  The list of SSL protocols to accept on the management console. A space-separated list of tokens in the format accepted by the Apache mod_ssl **SSLProtocol** directive.
  The default value is **all -SSLv2**.
- **ssl-ocsp-default-responder**
  Specifies the default responder URI for OCSP validation. The default is **http://localhost.localdomain**. The value for the default responder should always be preceded with **http://**.
- **ssl-ocsp-enable**
  Specifies OCSP validation of the client certificate chain. The default is **off**.
- **ssl-ocsp-override-responder**
  Specifies the force use of default responder URI for OCSP validation. The default is **off**.
- **ssl-ocsp-responder-timeout**
  Specifies the maximum allowable time in seconds for OCSP response. The default is 300 seconds.
- **ssl-ocsp-response-max-age**
  Specifies the maximum allowable age ("freshness") for OCSP responses. The default value (-1) does not enforce a maximum age, which means that OCSP responses are considered valid as long as their nextUpdate field is in the future.
- **ssl-ocsp-response-time-skew**
  Specifies the maximum allowable time skew in seconds for OCSP response validation. The default is 300 seconds.
- **ssl-verify-client**
  Specifies if the client certificate needs to be verified for SSL session establishment. The default is **no**.
- **ssl-verify-depth**
  Specifies maximum depth of CA certificates in client certificate verification. The default is **10**.

See Also

edit, *list*, *modify*, *show*, *tmsh*

hypervisor-info

Displays configuration information passed to a guest from the hypervisor.

Syntax

Access the **hypervisor-info** component within the **sys** module using the syntax in the following sections.

Display

```
show hypervisor-info
    (default | exa | gig | kil | meg | peta | raw | tera | yotta | zetta)
    field-fmt
```

Description

You can use the **hypervisor-info** component to display guest configuration information suggested by the hypervisor.

Examples

show hypervisor-info

Displays hypervisor configuration information in default units.

Options

For information about the options that you can use with the command **show**, see **help show**.

See Also

show, *tmsh*

icmp-stat

Displays and resets ICMP statistics on the BIG-IP system.

Syntax

Configure the **icmp-stat** component within the **sys** module using the syntax in the following section.

Modify

```
reset-stats icmp-stat
```

Display

```
show icmp-stat
    (default | exa | gig | kil | meg | peta | raw | tera | yotta | zetta)
```

Description

You can use the **icmp-stat** component to display and reset **ICMP** statistics. The statistics you can view are standard ICMP statistics, including ICMPv4 packets and errors, and ICMPv6 packets and errors.

Options

For information about the options that you can use with the command **show**, see **help show**.

For information about the options that you can use with the command **reset-stats**, see **help reset-stats**.

See Also

reset-stats, *show*, *icmp-stat*, *tmsh*

ip-address

Displays the IP addresses currently associated with a configuration object on a BIG-IP® system.

Syntax

Display the IP addresses associated with a BIG-IP system configuration object using the syntax in the following section.

Display

```
show ip-address
    [all-properties | field-fmt]
```

Description

You can use the **ip-address** component to display the location on the BIG-IP system of the IP addresses associated with a configuration object. The system displays the following information:

- **Entry**
  Displays the IP address and any associated configuration. For example, for a Local Traffic Manager pool member, the entry is the member's IP address and port number, **10.1.1.1:80**.
- **Component**
  Displays the type of component associated with the IP address. For example, for a Local Traffic Manager pool, the entry is **ltm pool**.
- **Object-ID**
  Displays the name of a configuration object associated with the IP address. For example, for a Local Traffic Manager pool named my_pool, the entry is **my_pool**.
- **Property**
  When you specify the **all-properties** option, displays the name of the property that contains the IP address value. Note that if the IP address is an object identifier the system displays **n/a**.

Examples

show ip-address

Displays the IP addresses currently associated with a BIG-IP system configuration object.

Options

For information about the options that you can use with the command **show**, see **help show**.

See Also

show, *tmsh*

ip-stat

Displays and resets IP statistics on the BIG-IP system.

Syntax

Configure the **ip-stat** component within the **sys** module using the syntax in the following section.

Modify

```
reset-stats ip-stat
```

Display

```
show ip-stat
    (default | exa | gig | kil | meg | peta | raw | tera | yotta | zetta)
```

Description

You can use the **ip-stat** component to display and reset **IP** statistics. The statistics you can view are standard IP statistics, including IPv4 and IPv6 packets, fragments, fragments reassembled, and errors.

Options

For information about the options that you can use with the command **show**, see **help show**.

For information about the options that you can use with the command **reset-stats**, see **help reset-stats**.

See Also

reset-stats, *show*, *ip-stat*, *tmsh*

iprep-status

Displays the status of an IP reputation database. In the BIG-IP(R) Configuration Utility, this database is referred to as the IP Address Intelligence database.

Syntax

Display information about the **iprep-status** component within the **sys** module using the following syntax.

Display

```
show iprep-status
    current-module
    field-fmt
    running-config
```

Description

You can use the **iprep-status** component to display status information about the IP reputation database. The reputation database (referred to as IP Address Intelligence in the Config Utility) is available from third-party vendors. An IP intelligence database is a list of IP addresses that have a questionable reputation. The status information returned includes:

```
- the date and time that the BIG-IP system last contacted the vendor server
- the date and time that the BIG-IP system last received an update
- the total number of IP address in the database
- the number of IP addresses in the most recent update
```

◆ Note

When the system has an IP Intelligence license and the database variable db iprep.autoupdate is enabled (default), the database is automatically downloaded and stored in the binary file:

```
/var/IpRep/F5IpRep.dat
```

The database contains information that maps IP addresses or ranges of IP addresses to one or more reputation categories. After every update, the IpRep data file is loaded from disk into the running configuration.

Examples

show iprep-status

Displays current status information for the IP reputation database.

Options

For information about the options that you can use with the command **show**, see **help show**.

See Also

show, *tmsh*

license

Manage the BIG-IP® system licensing information.

Syntax

Manage the **license** component within the **sys** module using the syntax in the following section.

Install

```
install license
    add-on-keys { [key] ...}
    license-server [ [host name] | [IP address] ]
    license-server-port [number]
    registration-key [key]
    verbose
```

Display

```
show license
    detail
```

Description

You can use the **license** component to do the following:

Display detailed licensing and version information for the system, including the registration key, licensing dates, platform ID, suggested service check date, and the installed active modules.

Install and update the system license.

Examples

show license

Displays the system software licensing information.

show license detail

Displays the system software licensing information, including optional modules and active features.

install license

Reactivate an existing license.

Options

- **add-on-keys**
  Specifies additional feature modules to be included in the license. If add-on keys are not specified the system will use the add-on keys in the current license file.
- **license-server**
  Specifies the host name or IP address of the license server. The default value is 65.61.115.202 (activate.f5.com).
- **license-server-port**
  Specifies the IP port of the license server. The default value is 443.
- **registration-key**
  Specifies the license registration key. If the registration key is not specified the system will use the registration key in the current license file.
- **verbose**
  Display status as the license is being installed.

For information about the options that you can use with the command **show**, see **help show**.

See Also

show, *tmsh*

log

Displays various system log files.

Syntax

Configure the **log** component within the **sys** module using the syntax in the following sections.

Display

```
show log
show log [audit | daemon | gtm | kernel | ltm | mail | messages |
  security | tmm | user | webui]
    lines [integer]
    range [date range]
```

Description

You can use the **log** component to display various logs.

Examples

show log

Displays a list of logs that you can view.

show log gtm

Displays the Global Traffic Manager log.

show log gtm lines 100 range 2/19/2006:15:04:00--epoch

Displays no more than 100 lines of the Global Traffic Manager log that were logged before the 19th of February 2006 at 3:04 pm.

Options

- **audit**
  Displays a log of configuration changes.
- **daemon**
  Displays the Unix daemon logs.
- **gtm**
  Displays the Global Traffic Manager logs.
- **kernel**
  Displays Linux Kernel messages.
- **lines**
  Specifies how many lines of the log that you want the system to display at one time.

- **ltm**
  Displays Local Traffic Manager logs.
- **mail**
  Displays mail daemon logs.
- **messages**
  Displays application messages.
- **range**
  Specifies the date range of the log information that you want the system to display.
- **security**
  Displays security-related messages.
- **tmm**
  Displays Traffic Manager Micro-kernel logs.
- **user**
  Displays various user process logs.
- **webui**
  Displays Configuration utility logs.

See Also

show, *tmsh*

log-rotate

Configures log rotation for the BIG-IP® system.

Syntax

Configure the **log-rotate** component within the **sys** module using the syntax in the following sections.

Modify

```
modify log-rotate
    common-backlogs [integer]
    common-include [string]
    description [string]
    include [string]
    max-file-size [integer]
    mysql-include [string]
    syslog-include [string]
    tomcat-include [string]
    wa-include [string]
edit log-rotate
    all-properties
    non-default-properties
```

Display

```
list log-rotate
list log-rotate [option]
show running-config log-rotate
show running-config log-rotate [option]
    all-properties
    non-default-properties
    one-line
```

Description

You can configure the system to rotate the log files after a specified length of time. This helps to clear the hard drive of unneeded log files.

Examples

modify log-rotate common-backlogs 7

Specifies that the system saves seven copies of the common log files.

list log-rotate all-properties

Displays the configuration of the **log-rotate** component.

Options

- **common-backlogs**
  Specifies the number of logs that you want the system to save. Select a number from the valid range of **1 - 100**. The default value is **24**.
- **common-include**
  The default value is **none**.

WARNING

*Do not use this option without assistance from the F5 Technical Support team. The system does not validate the commands issued using this option. If you use the **common-include** option incorrectly, you put the functionality of the system at risk.*

- **description**
  User defined description.
- **include**
  The default value is **none**.

WARNING

*Do not use this option without assistance from the F5 Technical Support team. The system does not validate the commands issued using this option. If you use the **include** option incorrectly, you put the functionality of the system at risk.*

- **max-file-size**
  The max size of rotated log files in kB. The default value is **1024**.
- **syslog-include**
  The default value is **none**.

WARNING

*Do not use this option without assistance from the F5 Technical Support team. The system does not validate the commands issued using this option. If you use the **syslog-include** option incorrectly, you put the functionality of the system at risk.*

- **tomcat-include**
  The default value is **none**.

WARNING

*Do not use this option without assistance from the F5 Technical Support team. The system does not validate the commands issued using this option. If you use the **tomcat-include** option incorrectly, you put the functionality of the system at risk.*

- **wa-include**
  The default value is **none**.

WARNING

*Do not use this option without assistance from the F5 Technical Support team. The system does not validate the commands issued using this option. If you use the **wa-include** option incorrectly, you put the functionality of the system at risk.*

See Also

edit, *list*, *modify*, *show*, *tmsh*

mac-address

Displays all MAC addresses currently associated with a configuration object on a BIG-IP® system, including all dynamically-discovered MAC addresses.

Syntax

Display the MAC addresses associated with a BIG-IP system configuration using the syntax in the following section.

Display

```
show mac-address
    field-fmt
```

Description

You can use the **mac-address** component to display the location on the BIG-IP system of the MAC addresses associated with a configuration object. The system displays the following information, which identifies the location of the MAC address in the configuration.

- **Entry**
  Displays the MAC address.
- **Component**
  Displays the type of component associated with the MAC address, for example, **net interface**.
- **Object-ID**
  Displays the name of a configuration object associated with the MAC address, for example, **2.1**.
- **Property**
  Displays the name of the property that contains the MAC address value. Note that if the MAC address is an object identifier the system displays **n/a**.

Examples

show mac-address

Displays all MAC addresses currently associated with a BIG-IP system configuration object.

Options

For information about the options that you can use with the command **show**, see **help show**.

See Also

show, *tmsh*

management-dhcp

Configures dhcp settings for the management interface (MGMT).

Syntax

Configure the **management-dhcp** component within the **sys** module using the syntax in the following sections.

Create/Modify

```
create management-dhcp [name]
modify management-dhcp [name]
  client-identifier [string]
  description [string]
  hostname [string]
  request-options [add | delete | modify | replace-all-with]
  send-options [add | delete | modify | replace-all-with]
edit management-dhcp [name]
    all-properties
```

Display

```
list management-dhcp
list management-dhcp [name]
show running-config management-dhcp
show running-config management-dhcp [name]
    all-properties
    one-line
```

Delete

```
delete management-dhcp [name]
```

Description

Specifies DHCP client settings for the management interface. These settings will be used to retrieve an IP address for the management interface if **mgmt-dhcp** is enabled.

Examples

modify management-dhcp default request-options add ntp-servers

Adds **ntp-servers** to the lists of options requested by the management interface DHCP client.

Options

- **client-id**
  Specifies the client identifier to send to the DHCP server.
- **description**
  User defined description.
- **hostname**
  Specifies the hostname to send to the DHCP server.
- **request-options**
  Specifies the options to request from the DHCP server.
- **send-options**
  Specifies the options to send to the DHCP server.

See Also

create, *delete*, *edit*, *list*, *modify*, *show*, *management-ip*, *management-route*, *tmsh*

management-ip

Configures the ip address and netmask for the management interface (MGMT).

Syntax

Configure the **management-ip** component within the **sys** module using the syntax in the following sections.

Create/Modify

```
create management-ip [ip address/netmask]
create management-ip [ip address/prefixlen]
modify management-ip [ip address/prefixlen]
  description
```

Display

```
list management-ip
show running-config management-ip
  all-properties
  one-line
```

Delete

```
delete management-ip [ip address/netmask]
delete management-ip [ip address/prefixlen]
```

Description

Specifies network settings for the management interface.

The management interface is available on all switch platforms and is designed for management purposes. You can access the browser-based Configuration utility and command line configuration utility through the management port. You cannot use the management interface in traffic management VLANs. You can configure only one IP address on the management interface.

After you make any changes using the **management-ip** component, issue the following command sequence to save the changes to the **bigip_base.conf** file: **save sys config**.

To configure management-ip firewall rules, see **security firewall management-ip-rules**.

Examples

create management-ip 10.2.3.4/255.255.0.0

Creates the IP address 10.2.3.4 on the management interface.

create management-ip 10.2.3.4/16

Creates the IP address 10.2.3.4 on the management interface.

Options

- **[ip address/netmask]**
  Specifies the IPv4 address and netmask.
- **[ip address/prefixlen]**
  Specifies the IPv6 address and prefixlen.
- **description**
  User defined description.
- **dhcp-enabled**
  Specifies if the ip address has been configured by DHCP.

See Also

create, *delete*, *list*, *modify*, *save*, *show*, *management-ip-rules*, *management-route*, *tmsh*

management-route

Configures route settings for the management interface (MGMT).

Syntax

Configure the **management-route** component within the **sys** module using the syntax in the following sections.

Create/Modify

```
create management-route [name | default | default-inet6]
modify management-route [name | default | default-inet6]
  description [string]
  gateway [ip address]
  mtu [number]
  network [ip address/netmask]
edit management-route [ [ [name | default | default-inet6]
                          | [glob] | [regex] ] ... ]
    all-properties
```

Display

```
list management-route
list management-route [ [ [name | default | default-inet6]
                          | [glob] | [regex] ] ... ]
show running-config management-route
show running-config management-route [ [ [name | default
                          | default-inet6] | [glob] | [regex] ] ... ]
    all-properties
    one-line
```

Delete

```
delete management-route [name]
```

Description

Specifies route settings for the management interface. You must configure a route on the management interface if you want to access the management network on the BIG-IP® system by connecting from another network.

The management interface is available on all switch platforms and is designed for management purposes. You can access the browser-based Configuration utility and command line configuration utility through the management port. You cannot use the management interface in traffic management VLANs.

Examples

create management-route default gateway 10.10.10.254

Sets the management interface default gateway IP address to 10.10.10.254.

create management-route myMgmtRoute network 10.10.10.0/24 gateway 10.10.10.254

Creates a management route named myMgmtRoute for the subnet 10.10.10.0/24 whose gateway IP address is 10.10.10.254.

modify management-route 10.10.10.0/24 gateway 172.24.74.62

Changes the management interface to subnet **10.10.10.0/24**, and the gateway to **172.24.74.62**.

Options

- **default**
  Specifies that the system forwards packets to the destination through the default IP address and netmask, **0.0.0.0 0.0.0.0**.
- **default-inet6**
  Specifies that the system forwards packets to the destination through the default version 6.0 IP address and netmask.
- **description**
  User defined description.
- **glob**
  Displays the items that match the **glob** expression. See **help glob** for a description of **glob** expression syntax.
- **[ip address/netmask]**
  Specifies the IP address and netmask through which the system forwards packets to the destination. You can use either of these formats: **0.0.0.0/0** or **0.0.0.0 0.0.0.0**.
- **gateway**
  Specifies that the system forwards packets to the destination through the gateway with the specified IP address.
- **mtu**
  Specifies the maximum transmission unit (MTU) for the management interface. The value of the MTU is the largest size that the BIG-IP system allows for an IP datagram passing through the management interface.
- **network**
  The subnet and netmask to be used for the route. This is an optional field; if empty the name should be of the form [ip address/netmask].
- **regex**
  Displays the items that match the regular expression. The regular expression must be preceded by an at sign (@[regular expression]) to indicate that the identifier is a regular expression. See **help regex** for a description of regular expression syntax.

See Also

create, *delete*, *edit*, glob, *list*, *modify*, regex, *show*, *management-ip*, *tmsh*

mcp-state

Displays information about the **mcpd** daemon.

Syntax

Display information about the **mcpd** daemon using **mcp-state** component within the **sys** module using the syntax in the following section.

Display

```
show mcp-state
    field-fmt
```

Description

You can use the **mcp-state** component to display the current state of the **mcpd** daemon.

Examples

show mcp-state

Displays, in a table, information about the state of the **mcpd** daemon.

show mcp-state field-fmt

Displays, in field format, information about the state of the **mcpd** daemon.

Options

For information about the options that you can use with the command **show**, see **help show**.

See Also

show, *tmsh*

memory

Displays system memory information and statistics.

Syntax

Configure the **memory** component within the **sys** module using the syntax in the following sections.

Display

```
show memory
    (default | exa | gig | kil | meg | peta | raw | tera | yotta | zetta)
    global
```

Description

You can use the **memory** component to display information about the system memory.

Examples

show memory gig

Displays memory statistics in gigabytes.

show memory raw

Displays raw memory statistics.

Options

For information about the options that you can use with the command **show**, see **help show**.

See Also

show, *tmsh*

ntp

Configures the Network Time Protocol (NTP) daemon for the BIG-IP® system.

Syntax

Configure the **ntp** component within the **sys** module using the following syntax.

Modify

```
modify ntp
    description [string]
    include [string]
    restrict [add | delete | replace-all-with] {
      [string] {
        address [IP address]
        default-entry [enabled | disable]
        description [string]
        ignore [enabled | disable]
        kod [enabled | disable]
        limited [enabled | disable]
        low-priority-trap [enabled | disable]
        mask [IP address]
        no-modify [enabled | disable]
        non-ntp-port [enabled | disable]
        no-peer [enabled | disable]
        no-query [enabled | disable]
        no-serve-packets [enabled | disable]
        no-trap [enabled | disable]
        no-trust [enabled | disable]
        ntp-port [enabled | disable]
        version [enabled | disable]
      }
    }
    restrict none
    servers [add | delete | replace-all-with] {
      [hostname | IP address] ...
    }
    servers none
    timezone [string]
edit ntp
    all-properties
    non-default-properties
```

Display

```
list ntp
list ntp [option]
show running-config ntp
show running-config ntp [option]
    all-properties
    non-default-properties
    one-line
```

Description

You can use this component to configure the NTP servers for the system.

Examples

modify ntp servers add {192.168.1.245}

Adds the NTP server with the IP address, **192.168.1.245**, to the system.

modify ntp servers replace-all-with {time.f5net.com}

Replaces the existing list of NTP servers with a single host, **time.f5net.com**.

modify ntp timezone "America/Los_Angeles"

Sets the system time to Pacific Standard Time.

modify ntp restrict add { basicrestrict { default-entry enable ignore enable } }

Adds a default restriction denying all packets.

Options

- **description**
  User defined description.
- **include**

WARNING

*Do not use this option without assistance from the F5 Technical Support team. The system does not validate the commands issued using the **include** option. If you use this option incorrectly, you put the functionality of the system at risk.*

- **restrict**
  Specifies a set of access restrictions.
  - **address**
    The address for the entry. See also, the **mask** option. The default value is **0.0.0.0**.
  - **default-entry**
    Specifies whether the entry is the default entry. The default value is **disabled**.
  - **description**
    User defined description.
  - **ignore**
    Specifies whether all packets will be ignored. The default value is **disabled**.

- **kod**
  Specifies whether a kod (kiss of death) packet will be sent when an access violation occurs. The default value is **disabled**.
- **limited**
  Specifies whether service will be denied if packet spacing limits are violated. The default value is **disabled**.
- **low-priority-trap**
  Specifies whether lower priority traps will be overridden by normal priority traps. The default value is **disabled**.
- **mask**
  The mask for the entry. See also, the **address** option. The default value is **0.0.0.0**.
- **no-modify**
  Specifies whether ntpq and ntpdc queries that attempt to modify the server are allowed. The default value is **disabled**.
- **non-ntp-port**
  When enabled, the restrict entry will be matched only if the source port is not the standard NTP UDP port (123). The default value is **disabled**.
- **no-peer**
  Specifies whether packets will be denied if they mobilize a new association. The default value is **disabled**.
- **no-query**
  Specifies whether ntpq and ntpdc queries will be denied. The default value is **disabled**.
- **no-serve-packets**
  Specifies whether all queries except ntpq and ntpdc will be denied. The default value is **disabled**.
- **no-trap**
  Specifies whether to decline the mode 6 control message trap service to matching hosts. The default value is **disabled**.
- **no-trust**
  Specifies whether to reject packets that are not cryptographically authenticated. The default value is **disabled**.
- **ntp-port**
  When enabled, the restrict entry will be matched only if the source port is the standard NTP UDP port (123). The default value is **disabled**.
- **version**
  Specifies whether packets will be rejected if they do not match the local NTP version. The default values is **disabled**.

◆ **servers**
Configures NTP servers for the BIG-IP system.

◆ **timezone**
Specifies the time zone that you want to use for the system time.

See Also

edit, *list*, *modify*, *show*, *tmsh*

outbound-smtp

Configures outgoing email for the BIG-IP® system.

Syntax

Configure the **outbound-smtp** component within the **sys** module using the following syntax.

Modify

```
modify outbound-smtp
    description [string]
    mailhub [string]
edit outbound-smtp
    all-properties
    non-default-properties
```

Display

```
list outbound-smtp
list outbound-smtp [option]
show running-config outbound-smtp
show running-config outbound-smtp [option]
    all-properties
    non-default-properties
    one-line
```

Description

You can use this component to configure the outgoing SMTP server that the system will use to send automated email.

Examples

modify outbound-smtp mailhub smtp.yoursite.com:587

Configures the TMOS system to send outgoing email through the specified SMTP server.

Options

- **description**
  User defined description.
- **mailhub**
  The SMTP server to use to send outgoing automated email.

See Also

edit, *list*, *modify*, *tmsh*

proc-info

Display CPU and memory usage for each process.

Syntax

Display **proc-info** component within the **sys** module using the syntax in the following section.

Display

```
show proc-info
show proc-info process_name
    (default | field-fmt | all | kil | meg | gig | raw | exa | peta | tera | zetta |
yotta)
```

Description

Show proc-info displays CPU and memory usage for each process and the process associated module name. This can be used to debug which process or module uses more resource.

Options

For information about the options that you can use with the command **show**, see **help show**.

See Also

show, *tmsh*

provision

Configures provisioning on the BIG-IP® system.

Syntax

Configure the **provision** component within the **sys** module using the syntax in the following sections.

Modify

```
modify provision [afm | am | apm | asm | avr | fps | gtm | lc | ltm | pem | swg]
    cpu-ratio [integer]
    disk-ratio [integer]
    level [custom | dedicated | minimum | nominal | none]
    memory-ratio [integer]

edit provision
  [ [ [afm | am | apm | asm | avr | fps | gtm | lc | ltm | pem | swg] |
      [glob] | [regex] ] ... ]
    all-properties
    non-default-properties
```

Display

```
list provision
  [ [ [afm | am | apm | asm | avr | fps | gtm | lc | ltm | pem | swg] |
      [glob] | [regex] ] ... ]
show running-config provision
  [ [ [afm | am | apm | asm | avr | fps | gtm | lc | ltm | pem | swg] |
      [glob] | [regex] ] ... ]
    all-properties
    non-default-properties
    one-line
```

Description

You can use the **provision** component to modify the allocation of resources to the licensed modules on your system.

Examples

- **modify provision asm level minimum**
  Provisions the minimum amount of resources for the BIG-IP Application Security Manager.
- **list provision**
  Displays the current provisioning of the system.
  - **create transaction**

- **modify / sys provision ltm level minimum**
- **modify / sys provision gtm level nominal**
- **submit transaction**

The previous four steps create a transaction to modify the provisioning of a unit to provision the Local Traffic Manager at the **minimum** level and the Global Traffic Manager at the **nominal** level.

- **create transaction**
- **modify / sys provision ltm level none**
- **modify / sys provision gtm level dedicated**
- **submit transaction**

The previous four steps create a transaction to modify the provisioning of a unit on which the Local Traffic Manager is currently provisioned at the **nominal** level, and we want to dedicate all of the unit's resources to the Global Traffic Manager.

Options

- **all**
  Specifies that you are provisioning all of the available modules.
- **afm**
  Specifies that you are provisioning the BIG-IP Advanced Firewall Manager. When the Advanced Firewall Manager is provisioned, the **tmsh** module **afm** is enabled.
- **am**
  Specifies that you are provisioning the BIG-IP Acceleration Manager. When the Acceleration Manager is provisioned, the **tmsh** module **am** is enabled.
- **apm**
  Specifies that you are provisioning the BIG-IP Access Policy Manager. When the Access Policy Manager is provisioned, the **tmsh** module **apm** is enabled.
- **asm**
  Specifies that you are provisioning the BIG-IP Application Security Manager. When **asm** is provisioned the **tmsh** module **asm** is enabled.
- **avr**
  Specifies that you are provisioning the BIG-IP Application Visibility and Reporting. When Application Visibility and Reporting is provisioned the **tmsh** module **avr** is enabled.

- **cpu-ratio**
  Use this option only when the **level** option is set to **custom**. F5 Networks recommends that you do not modify this option. The default value is **none**.
- **disk-ratio**
  Use this option only when the **level** option is set to **custom**. F5 Networks recommends that you do not modify this option. The default value is **none**.
- **fps**
  Specifies that you are provisioning the BIG-IP Fraud Protection Service. When **fps** is provisioned the **tmsh** module **fps** is enabled.
- **glob**
  Displays the items that match the **glob** expression. See **help glob** for a description of **glob** expression syntax.
- **gtm**
  Specifies that you are provisioning the BIG-IP Global Traffic Manager. When **gtm** is provisioned the **tmsh** module **gtm** is enabled.
- **lc**
  Specifies that you are provisioning the BIG-IP Link Controller. When Link Controller is provisioned the **tmsh** module **lc** is enabled.
- **level**
  Specifies the level of resources that you want to provision for a module. The options are:
  - **custom**
    F5 Networks does not recommend that you specify this level.
  - **dedicated**
    Specifies that all resources are dedicated to the module you are provisioning. For all other modules, the **level** option must be set to **none**.
  - **minimum**
    Specifies that you want to provision the minimum amount of resources for the module you are provisioning.
  - **nominal**
    Specifies that you want to share all of the available resources equally among all of the modules that are licensed on the unit.
  - **none**
    Specifies that you do not want to provision any resources for this module.
- **ltm**
  Specifies that you are provisioning the BIG-IP Local Traffic Manager.
- **memory-ratio**
  Use this option only when the **level** option is set to **custom**. F5 Networks recommends that you do not modify this option. The default value is **none**.

- **pem**
  Specifies that you are provisioning the BIG-IP Policy Enforcement Manager. When Policy Enforcement Manager is provisioned the **tmsh** module **pem** is enabled.
- **regex**
  Displays the items that match the regular expression. The regular expression must be preceded by an at sign (@[regular expression]) to indicate that the identifier is a regular expression. See **help regex** for a description of regular expression syntax.
- **swg**
  Specifies that you are provisioning the BIG-IP Secure Web Gateway. When Secure Web Gateway is provisioned the **tmsh** components **apm url-filter** and **apm swg-scheme** are enabled.

See Also

edit, glob, *list*, *modify*, regex, *show*, *tmsh*

pva-traffic

Displays and resets Packet Velocity® ASIC (PVA) traffic statistics for the system.

Syntax

Configure the **pva-traffic** component within the **sys** module using the following syntax.

Modify

```
reset-stats pva-traffic
```

Display

```
show pva-traffic
    (default | exa | gig | kil | meg | peta | raw | tera | yotta | zetta)
    global
```

Description

You can use the **pva-traffic** component to display traffic statistics, including bits in and out, packets in and out, current, maximum, and total connections, and other miscellaneous statistics.

The BIG-IP® system has one PVA accelerator; however, when you run the command **show pva-traffic**, the system displays a PVA statistics entry for each Traffic Management Microkernel (TMM).

Examples

show pva-traffic

Displays PVA traffic statistics for the system.

show pva-traffic raw

Displays PVA traffic statistics for the system in raw data form.

Options

For information about the options that you can use with the command **show**, see **help show**.

For information about the command **reset-stats**, see **help reset-stats**.

See Also

reset-stats, *show*, *tmm-traffic*, *traffic*, *tmsh*

scriptd

Configure the scriptd daemon

Syntax

Configure the **scriptd** daemon within the **sys** module using the syntax in the following sections.

Modify

```
modify scriptd
    log-level [alert | crit | debug | emerg | err | info | notice | warn]
    max-script-run-time [seconds]
```

Display

```
list scriptd
show running-config scriptd
    all-properties
```

Description

You can use the **scriptd** component to configure the scriptd daemon. The scriptd daemon runs app application template implementation scripts when an application service is created or updated (see **sys application template** and **sys application service**).

Examples

list scriptd

Displays **scriptd** configuration.

modify scriptd max-script-run-time 120

Updates the maximum time, in seconds, that a script is allowed to run.

Options

- **log-level**
  Specifies the syslog level at which **scriptd** will generate log messages.
- **max-script-run-time**
  Specifies, in seconds, the maximum amount of time that a script is allowed to run before **scriptd** will kill the script. The default value is **300**. The minimum value is **5**.

See Also

list, *modify*, *show*, *template*, *service*, *tmsh*

service

Manages services on the BIG-IP® system.

Syntax

Configure the **service** component within the **sys** module using the syntax in the following sections.

Modify

```
modify service [name]
    [add | disable | enable | reinit | remove]
restart service [name]
start service [name]
stop service [name]
    force
```

Display

```
list service
list service [name]
show running-config service
show running-config service [name]
  all-properties
show service
  memstat
```

Description

You can use the **service** component to add, disable or enable, start, stop, restart, reinitialize, remove, or display information about a service.

Note that the **tmsh** connection to **mcpd** will be dropped if you stop or restart the **mcpd** service. The next **tmsh** command will prompt you to try again. Alternatively you can quit **tmsh** and login again.

Examples

list service

Displays information about the services available on the BIG-IP system.

restart service mcpd

Restarts the **mcpd** daemon.

Options

- **add**
  Adds the specified service.
- **disable**
  Disables the specified service.
- **enable**
  Enables the specified service.
- **memstat**
  Displays memory usage statistics for the specified service.
- **reinit**
  Reinitializes the specified service.
- **remove**
  Removes the specified service.

See Also

list, *modify*, *restart*, *show*, *start*, *stop*, *tmsh*

smtp-server

Configure the SMTP server connection.

Syntax

Create or modify an SMTP server access configuration using the syntax in the following sections.

Create / Modify

```
modify smtp-server [name]
create smtp-server [name]
    app-service [[string] | none]
    [authentication-enabled | authentication-disabled]
    encrypted-connection [none | tls | ssl]
    local-host-name [string]
    smtp-server-host-name [string]
    smtp-server-port [integer]
    from-address [string]
    username [string]
    password [string]
```

Display

```
list smtp-server
show running-config smtp-server
    all-properties
```

Description

You can use the **smtp-server** component to configure an SMTP server connection.

Examples

list smtp-server

Displays the SMTP configuration.

modify smtp-server smtp1 authentication-enabled encrypted-connection ssl local-host-name example.f5.com from-address example@f5.com smtp-server-host-name mail.server.com username user password pass

Configures SMTP server connection with **username=user** and **password=pass** to be authenticated against the SMTP server **mail.server.com**. SSL encryption will be used for all communication with the SMTP server. Email messages will be sent out with the address **example@f5.com** in the "Reply-To" address.

Options

- **app-service**
  Specifies the name of the application service to which the object belongs. The default value is **none**. **Note:** If the **strict-updates** option is **enabled** on the application service that owns the object, you cannot modify or delete the object. Only the application service can modify or delete the object.
- **[authentication-enabled | authentication-disabled]**
  Enables or disables authentication against the configured SMTP server.
- **encrypted-connection**
  Specifies which type of encrypted connection the SMTP server requires in order to send mail. The default value is **none**.
- **local-host-name**
  Specifies the host name used in SMTP headers in the format of a fully qualified domain name. This setting does not refer to the BIG-IP system's Hostname.
- **smtp-server-host-name**
  Specifies the SMTP server host name in the format of a fully qualified domain name.
- **smtp-server-port**
  Specifies the SMTP port number. The default value is **25**.
- **from-address**
  Specifies the email address that the email is being sent from. This is the "Reply-to" address that the recipient sees.
- **username**
  Specifies the user name that the SMTP server requires when validating a user.
- **password**
  Specifies the password that the SMTP server requires when validating a user. This password is stored in an encrypted form.

See Also

list, *create*, *modify*, *show*, *tmsh*

snmp

Configures the simple network management protocol (SNMP) daemon for the BIG-IP® system.

Syntax

Configure the **snmp** component within the **sys** module using the following syntax.

Modify

```
modify snmp
    agent-addresses [add | delete | replace-all-with] {
      ["agent:port"] ...
    }
    agent-addresses none
    agent-trap [enabled | disabled]
    allowed-addresses [add | delete | replace-all-with] {
      [IP address]
    }
    allowed-addresses none
    auth-trap [enabled | disabled]
    bigip-traps [enabled | disabled]
    communities [add | delete | modify | replace-all-with] {
      [name] {
        access [ro | rw]
        community-name [string]
        description [string]
        ipv6 [enabled | disabled]
        oid-subset [string]
        source [ default | [string] ]
      }
    }
    communities none
    description [string]
    disk-monitors [add | delete | modify | replace-all-with] {
      [name] {
        description [string]
        minspace [integer]
        minspace-type [percent | size]
        path [string]
      }
    }
    disk-monitors none
    include [string]
    l2forward-vlan [all | add | delete | replace-all-with] {
      [VLAN name] ...
    }
    l2forward-vlan none
    load-max1 [integer]
    load-max5 [integer]
    load-max15 [integer]
    process-monitors [add | delete | modify | replace-all-with] {
      [name] {
        description [string]
        process [string]
```

```
    min-processes [integer]
    max-processes [ [integer] | infinity ]
  }
}
process-monitors none
sys-contact [string]
sys-location [string]
sys-services [integer]
trap-community [string]
trap-source [IP address]
traps [add | delete | modify | replace-all-with] {
  [name] {
    auth-password [string]
    auth-protocol [md5 | sha | none]
    community [string]
    description [string]
    engine-id [ [number] | none ]
    host [ [ip address] | [FQDN] | [ [protocol]:[ip address] ] |
           [ [protocol]:[FQDN] ] ]
    port [integer]
    privacy-password [string]
    privacy-protocol [aes | des | none]
    security-level [auth-no-privacy | auth-privacy | no-auth-no-privacy]
    security-name [string]
    version [1 | 2c | 3]
  }
}
traps none
users [add | delete | modify | replace-all-with] {
  [user name] {
    access [ro | rw]
    auth-password [string]
    auth-protocol [md5 | sha | none]
    description [string]
    oid-subset [string]
    privacy-password [string]
    privacy-protocol [aes | des | none]
    security-level [auth-no-privacy | auth-privacy | no-auth-no-privacy]
    username [string]
  }
}
users none
v1-traps [add | delete | modify | replace-all-with] {
  [name] {
    community [string]
    description [string]
    host [ [ip address] | [FQDN] | [ [protocol]:[ip address] ] |
           [ [protocol]:[FQDN] ] ]
    port [integer]
  }
}
v1-traps none
v2-traps [add | delete | modify | replace-all-with] {
  [name] {
    community [string]
    description [string]
    host [ [ip address] | [FQDN] | [ [protocol]:[ip address] ] |
           [ [protocol]:[FQDN] ] ]
    port [integer]
  }
}
v2-traps none
```

```
edit snmp
    all-properties
    non-default-properties
```

Display

```
list snmp
list snmp [option]
show running-config snmp
show running-config snmp [option]
    all-properties
    non-default-properties
    one-line
```

Description

You can use the **snmp** component to configure the **snmpd** daemon for the BIG-IP system.

Important

*F5 Networks recommends that users of the Configuration utility exit the utility before changes are made to the system using the command sequence **tmsh sys snmp**. This is because making changes to the system using this command causes a restart of the **snmpd** daemon. Likewise, restarting the **snmpd** daemon creates the necessity for a restart of the Configuration utility.*

Examples

modify snmp sys-contact admin@company.com

Modifies the configuration to indicate that the person who administers the **snmpd** daemon for the system can be reached using the email address, admin@company.com.

modify snmp sys-location "central office"

Modifies the configuration to indicate that the physical location of the system is the central office.

modify snmp agent-trap disabled

Disables agent traps.

modify snmp allowed-addresses add {10.10.0.0/255.255.240.0}

Adds a range of SNMP clients to the **/etc/hosts.allow** file.

modify snmp traps add { tv1 { version 1 community public host 192.168.1.240 port 162 } }

Adds an SNMP version 1 trapsess, **tv1**, to the system. The destination IP address of **tv1** is **192.168.1.240**, the port is **162**, and the community that has access to **tv1** is **public**. The default port is **162**.

modify snmp traps add { tv2 {version 2c community public host 192.168.1.241 port 162} }

Adds an SNMP version 2 trapsess, **tv2**, to the system. The destination IP address of **tv2** is **192.168.1.241**, the port is **162**, and the community that has access to **tv2** is **public**. The default port is **162**. The default version is 2c (version 2).

modify snmp traps add { trap_v3_1 { version 3 host 192.168.1.242 port 162 security-level auth-no-privacy security-name mySecurityName auth-protocol md5 auth-password myAuthPassword } }

Adds an SNMP version 3 trapsess, **trap_v3_1**, with authentication capabilities to the system. The destination IP address of **trap_v3_1** is **192.168.1.242**, the port is **162**, the security level is the authentication without privacy, the security name is **mySecurityName**, the authentication protocol is **MD5**, and the authentication password is **myAuthPassword**. The default port is **162**.

modify snmp traps add { trap_v3_2 { version 3 host 192.168.1.243 port 162 security-level auth-privacy security-name mySecurityName auth-protocol sha auth-password myAuthPassword privacy-protocol aes privacy-password myPrivacyPassword } }

Adds an SNMP version 3 trapsess, **trap_v3_2**, with authentication and privacy capabilities to the system. The destination IP address of **trap_v3_2** is **192.168.1.243**, the port is **162**, the security level is the authentication and privacy, the security name is **mySecurityName**, the authentication protocol is **SHA**, the authentication password is **myAuthPassword**, the privacy protocol is **AES**, and the privacy password is **myPrivacyPassword**. The default port is **162**.

modify snmp v1-traps add { ts { community public host 10.20.5.11 port 162 } }

Adds an SNMP version 1 trapsink, **ts**, to the system. The destination IP address of **ts** is **10.20.5.11**, the port is **162**, and the community that has access to **ts** is **public**. The default port is **162**.

modify snmp v2-traps add { t2s { community public host 10.20.5.12 port 162 } }

Adds an SNMP version 2 trap2sink, **t2s**, to the system. The destination IP address of **t2s** is **10.20.5.12**, the port is **162**, and the community that has access to **t2s** is **public**. The default port is **162**.

modify snmp users add { myUser1 { username myUser1 access ro security-level auth-no-privacy auth-protocol md5 auth-password myAuthPassword privacy-protocol none } }

Adds an SNMP version 3 user with the user name, **myUser1**, to the system. The access to the management information base (MIB) of **myUser1** is read-only, the security level is the authentication without privacy, the authentication protocol is **MD5**, and the authentication password is **myAuthPassword**.

modify snmp users add { myUser2 { username myUser2 oid-subset .1.3.6.1.4.1.3375 auth-protocol md5 auth-password myAuthPassword privacy-protocol none } }

Adds an SNMP version 3 user with the user name, **myUser2**, to the system. The access to the management information base (MIB) of **myUser2** is read-only (by default) and restricted to every object below .1.3.6.1.4.1.3375 object identifier in the MIB tree, the security level is the authentication without privacy, the authentication protocol is **MD5**, and the authentication password is **myAuthPassword**.

modify snmp users add { myUser3 { username myUser3 access ro security-level auth-privacy auth-protocol sha auth-password myAuthPassword privacy-protocol des privacy-password myPrivacyPassword } }

Adds an SNMP version 3 user with the user name, **myUser3**, to the system. The access to the management information base (MIB) of **myUser3** is read-only, the security level is the authentication and privacy, the authentication protocol is **SHA**, the authentication password is **myAuthPassword**, the privacy protocol is **DES**, and the privacy password is **myPrivacyPassword**.

modify snmp users add { myUser4 { username myUser4 access ro security-level no-auth-no-privacy auth-protocol none privacy-protocol none } }

Adds an SNMP version 3 user with the user name, **myUser4**, to the system. The access to the management information base (MIB) of **myUser4** is read-only without the authentication and privacy settings.

modify snmp communities add { community1 { community-name mycommunity access ro source 192.168.1.246 oid-subset 5 ipv6 disabled } }

Creates a community specification named **community1** for the BIG-IP system. community1 includes a community, named **mycommunity**, that provides read-only access to the host at **192.168.1.246**. This host cannot be an IPv6 address. The oid for this community is **5**.

modify snmp communities add { new-name { community-name public source default oid-subset 1 access ro } }

Replaces the default community specification for the BIG-IP system. Using this command, the default community includes a community, named **public**, that provides read-only access to the default host. The oid for this community is **1**.

modify snmp communities delete { mycommunity }

Deletes the community named **mycommunity**.

modify snmp load-max1 0 load-max5 0 load-max15 0

Disables monitoring of snmpd load average on the BIG-IP system.

Options

- **agent-addresses**
  Indicates that the SNMP agent is to listen on the specified address. F5 Networks recommends that you do not change this setting without fully understanding the impact of the change.

- **agent-trap**
  Specifies, when **enabled**, that the **snmpd** daemon sends traps, for example, start and stop traps. The default value is **enabled**.
- **allowed-addresses**
  Configures the IP addresses of the SNMP clients from which the **snmpd** daemon accepts requests. An SNMP client is a system that runs the SNMP manager software for the purpose of remotely managing the BIG-IP system. The default value is **127**.
- **auth-trap**
  Specifies, when **enabled**, that the **snmpd** daemon generates authentication failure traps. The default value is **disabled**.
- **bigip-traps**
  Specifies, when **enabled**, that the BIG-IP system sends device warning traps to the trap destinations. The default value is **enabled**.
- **community**
  Configures a community for the **snmpd** daemon. Note that you must include a community key, and you must enclose the attributes in braces. The options are additive and include:
  - **access**
    Specifies the community access level to the MIB. The access options are **ro** (read-only) or **rw** (read-write). The default value is **ro**.
  - **community name**
    Specifies the name of the community that you are configuring for the **snmpd** daemon. This option is required. The default value is **public**.
  - **description**
    User defined description.
  - **ipv6**
    Specifies to enable or disable IPv6 addresses for the community that you are configuring. The default value is **disabled**.
  - **oid-subset**
    Specifies to restrict access by the community to every object below the specified object identifier (OID).
  - **source**
    Specifies the source addresses with the specified community name that can access the management information base (MIB). The default value is **default**, which means allow any source address to access the MIB.
- **description**
  User defined description.
- **disk-monitors**
  Checks the disks mounted at the specified path for available disk space. The options are:
  - **description**
    User defined description.
  - **minspace**
    Specifies the minimum disk space threshold in either kBs or percentage based on the value of the **minspace-type** option. If the

available disk space is less than this amount, the associated entry in the 1.3.6.1.4.1.2021.9.1.100 MIB table is set to **(1)** and a descriptive error message is returned to queries of **1.3.6.1.4.1.2021.9.1.101**.

- **minspace-type**
  Specifies a minimum disk space measurement type of either size in kB, or percent. Note that the value of the **minspace** option is based on the value of this option.
- **path**
  Specifies the path to the disk that the system checks for disk space. This option is required.

◆ **include**
Warning: Do not use this parameter without assistance from the F5 Technical Support team. The system does not validate the commands issued using the include parameter. If you use this parameter incorrectly, you put the functionality of the system at risk.

◆ **l2forward-vlan**
Specifies the VLANs for which you want the **snmpd** daemon to expose Layer 2 forwarding information. Layer 2 forwarding is the means by which frames are exchanged directly between hosts, with no IP routing required. The default value is **none**.
The options are:

- **all**
  The **snmpd** daemon exposes Layer 2 forwarding information for all VLANS.

WARNING

When you set this option to all, the system can create a very large table of statistics and potentially affect system performance.

- **none**
  Indicates that this option is not set.

Important

*The default is not the same as setting this option to the string "none," which indicates that you do not want the **snmpd** daemon to expose Layer 2 forwarding for any VLAN.*

- **VLAN name**
  Specifies the names of the VLANs for which the **snmpd** daemon exposes Layer 2 forwarding information. The **snmpd** daemon overwrites the value of the **sysL2ForwardAttrVlan object** identifier (OID) with the specified VLAN names. Once you set this parameter, users cannot change the value of the **sysL2FowardAttrVlan** OID using the SNMP set method.

◆ **load-max1**
Specifies the maximum 1-minute load average of the machine. If the load exceeds this threshold, the associated entry in the 1.3.6.1.4.1.2021.10.1.100 MIB table is set to **(1)** and a descriptive error

message is returned to queries of **1.3.6.1.4.1.2021.10.1.101**.
Note that when you specify a **0** (zero) for all three of the **load-max1**, **load-max5**, and **load-max15** options, the system does not monitor the load average.

- **load-max5**
  Specifies the maximum 5-minute load average of the machine. If the load exceeds this threshold, the associated entry in the 1.3.6.1.4.1.2021.10.1.100 MIB table is set to (1) and a descriptive error message is returned to queries of 1.3.6.1.4.1.2021.10.1.101.
  Note that when you specify a **0** (zero) for all three of the **load-max1**, **load-max5**, and **load-max15** options, the system does not monitor the load average.
- **load-max15**
  Specifies the maximum 15-minute load average of the machine. If the load exceeds this threshold, the associated entry in the 1.3.6.1.4.1.2021.10.1.100 MIB table is set to (1) and a descriptive error message is returned to queries of 1.3.6.1.4.1.2021.10.1.101.
  Note that when you specify a **0** (zero) for all three of the **load-max1**, **load-max5**, and **load-max15** options, the system does not monitor the load average.
- **process-monitors**
  Specifies to check the machine to determine if the specified process is running. An error flag (1) and a description message are passed to the 1.3.6.1.4.1.2021.2.1.100 and 1.3.6.1.4.1.2021.2.1.101 MIB columns (respectively) if the specified program is not found in the process table as reported by /bin/ps -e.
  F5 Networks recommends that you do not modify or delete system processes; however, you can add, modify, or delete user-defined processes.
  The options are:
  - **description**
    User defined description.
  - **max-processes**
    Specifies the maximum number of instances of the process that can run. The default value is **1**.
    If you do not specify values for the **min-processes** and **max-processes** options, the **max-processes** option is **1** by default.
  - **min-processes**
    Specifies the minimum number of instances of the process that can run. The default value is **1**.
    If you do not specify a value for the **max-processes** option, and the **min-processes** option is not specified, the **min-processes** option is **0** (zero) by default.
  - **process**
    Specifies the name of the monitored process. The maximum length for a process name is 16 characters. This option is required.

- **sys-contact**
  Specifies the name of the person who administers the **snmpd** daemon for this system. The default value is **"Customer Name<admin@customer.com"**.

◆ Note

*If you enter a string that contains spaces, you must enclose the string in quotation marks and use back slashes to escape the quotation marks (for example, **"John Doe"**).*

- **sys-location**
  Describes this system's physical location. The default value is **Network Closet 1**.

◆ Note

*If you enter a string that contains spaces, you must enclose the string in quotation marks and use back slashes to escape the quotation marks (for example, **"Engineering Lab"**).*

- **sys-services**
  Specifies the value of the system.sysServices.0 object. The default value is **78**.
- **trap-community**
  Specifies the community name for the trap destination. The default value is **public**.
- **traps**
  Configures the SNMP version 1, version 2, or version 3 trap destination. Note that you must include a trapsess key, and you must enclose the attributes in braces.
  The options are additive and include:
  - **auth-password**
    Specifies the authentication password, which must be at least eight characters long. This option is valid only for SNMP version 3. If you enter the authentication password, the value of the **auth-protocol** option cannot be set to **none**.
  - **auth-protocol**
    Specifies the authentication method to use to deliver the trap message. The default value is **none**.
    You can specify the following authentication methods:
    - **md5**
      The system uses the message digest algorithm (MD5) to authenticate the trap message. This value is valid only for SNMP version 3.
    - **none**
      The system does not authenticate the trap message. Note that if you use this value, you cannot use the **auth-password** option. This value is invalid for SNMP version 3.

  - **sha**
    The system uses the secure hash algorithm (SHA) to authenticate the trap message. This option is valid only for SNMP version 3.
- **community**
  Specifies a community that has access to the trap message. This option is required for SNMP version 1 and version 2 only.
- **description**
  User defined description.
- **engine-id**
  Specifies the unique authoritative security engine ID. This option is valid only for SNMP version 3. The default value is **none**. You can find the engine ID generated by the SNMP agent at /config/net-snmp/snmpd.conf on the BIG-IP system. Note that it is identified as oldEngineID in this file.
- **host**
  Specifies the trap destination that you are configuring, the IP address, FQDN, or either of these with an embedded protocol, for example tcp:10.10.10.1 or tcp:www.f5.com. Note that you must configure the DNS Server on the BIG-IP system. You can use the command **sys dns** to do this. This option is required.
- **port**
  Specifies the port for the trap destination that you are configuring. The default value is **162**.
- **privacy-password**
  Specifies the privacy password, which must be at least eight characters long. This option is valid only for SNMP version 3. If you enter the privacy password, the value of the **privacy-protocol** option cannot be set to **none**.
- **privacy-protocol**
  Specifies the encryption/privacy method to use to deliver the trap message. The default value is **none**.
  You can specify the following privacy methods:
  - **aes**
    The system encrypts the trap message using Advanced Encryption Standard (AES). This value is valid only for SNMP version 3.
  - **des**
    The system encrypts the trap message using Data Encryption Standard (DES). This value is valid only for SNMP version 3.
  - **none**
    The system does not encrypt the trap message. Note that if you use this value, you cannot use the **privacy-password** option.
- **security-level**
  Specifies the security level to use to deliver the trap message. The default value is **no-auth-no-privacy**.
  You can specify the following security levels:

- **no-auth-no-privacy**
  Provides no authentication and no encryption for the trap message. This value is invalid for SNMP version 3.
- **auth-no-privacy**
  Provides the authentication without encryption for the trap message. Specifies to use the value of the **auth-protocol** option, but not the value of the **privacy-protocol** option. Note that if you use this option, the value of the **auth-protocol** option cannot be set to **none**, and you must configure a value for the **auth-password** option. This value is valid only for SNMP version 3.
- **auth-privacy**
  Provides the authentication and encryption for the trap message. Specifies to use the value of the **auth-protocol** and **privacy-protocol** options. Note that if you use this option, the value of the **auth-protocol** and **privacy-protocol** options cannot be set to **none**, and you must configure a value for the **auth-password** and **privacy-password** options. This option is valid only for SNMP version 3.

- **security-name**
  Specifies the security name the system uses to handle SNMP version 3 trap message. The default value is **none**. This option is required for SNMP version 3.
- **version**
  Specifies the security model to use. The options are **1** (version 1), **2c** (version 2), or **3** (version 3). The default value is **2c**.

◆ **trap-source**
Specifies the source of the SNMP trap. The default value is **none**.

◆ **users**
Configures the users for which you are setting an SNMP version 3 access. Note that you must include a user key, and you must enclose the attributes in braces.
The options are additive and include:

- **access**
  Specifies the user access level to the management information base (MIB). The access options are **ro** (read-only) or **rw** (read-write). The default value is **ro**.
- **auth-password**
  Specifies the authentication password, which must be at least eight characters long. If you enter the authentication password, the value of the **auth-protocol** option cannot be set to **none**.
- **auth-protocol**
  Specifies the authentication method to use to deliver the SNMP message. This option is required.
  You can specify the following authentication methods:
  - **md5**
    The system uses the message digest algorithm (MD5) to authenticate the SNMP message.

- **none**
  The system does not authenticate the SNMP message. Note that if you use this value, you should set the **security-level** to **no-auth-no-privacy** and you cannot use the **auth-password** option.
- **sha**
  The system uses the secure hash algorithm (SHA) to authenticate the SNMP message.

- **description**
  User defined description.
- **oid-subset**
  Specifies to restrict access by the user to every object below the specified object identifier (OID).
- **privacy-password**
  Specifies the privacy password, which must be at least eight characters long. If you enter the privacy password, the value of the **privacy-protocol** option cannot be set to **none**.
- **privacy-protocol**
  Specifies the encryption/privacy method to use to deliver the SNMP message. This option is required.
  You can specify the following encryption methods:
  - **aes**
    The system encrypts the SNMP message using Advanced Encryption Standard (AES).
  - **des**
    The system encrypts the SNMP message using Data Encryption Standard (DES).
  - **none**
    The system does not encrypt the SNMP message. Note that if you use this value, you cannot use the **privacy-password** option.
- **security-level**
  Specifies the security level to use to deliver the SNMP message.
  You can specify the following security levels:
  - **no-auth-no-privacy**
    Provides no authentication and no encryption for the SNMP message.
  - **auth-no-privacy**
    Provides the authentication without encryption for the SNMP message. Specifies to use the value of the **auth-protocol** option, but not the value of the **privacy-protocol** option. Note that if you use this option, the value of the **auth-protocol** option cannot be set to **none**, and you must configure a value for the **auth-password** option.
  - **auth-privacy**
    Provides the authentication and encryption for the SNMP message. Specifies to use the value of the **auth-protocol** and **privacy-protocol** options. Note that if you use this option, the

value of the **auth-protocol** and **privacy-protocol** options cannot be set to **none**, and you must configure a value for the **auth-password** and **privacy-password** options.

- **username**
  Specifies the name of the user who is using SNMP version 3 to access the management information base (MIB). This option is required.

◆ **v1-traps**
Configures an SNMP version 1 trap destination. Note that you must include a version 1 trapsink key, and you must enclose the attributes in braces.
The options are additive and include:

- **community**
  Specifies the community name for the trap destination that you are configuring. This option is required.
- **description**
  User defined description.
- **host**
  Specifies the trap destination that you are configuring, the IP address, FQDN, or either of these with an embedded protocol, for example tcp:10.10.10.1 or tcp:www.f5.com. Note that you must configure the DNS Server on the BIG-IP system. You can use the command **sys dns** to do this. This option is required.
- **port**
  Specifies the port for the trap destination that you are configuring. The default value is **162**.

◆ **v2-traps**
Configures an SNMP version 2 trap destination. Note that you must include a version 2 trap2sink key, and you must enclose the attributes in braces.
The options are additive and include:

- **community**
  Specifies the community name for the trap destination that you are configuring. This option is required.
- **description**
  User defined description.
- **host**
  Specifies the trap destination that you are configuring, the IP address, FQDN, or either of these with an embedded protocol, for example tcp:10.10.10.1 or tcp:www.f5.com. Note that you must configure the DNS Server on the BIG-IP system. You can use the command **sys dns** to do this. This option is required.
- **port**
  Specifies the port for the trap destination that you are configuring. The default value is **162**.

See Also

create, *delete*, *edit*, *list*, *modify*, *show*, *tmsh*

sshd

Configures the Secure Shell (SSH) daemon for the BIG-IP® system.

Syntax

Configure the **sshd** component within the **sys** module using the syntax in the following sections.

Modify

```
modify sshd
    allow [add | delete | replace-all-with] {
      [ [hostname] | [IP address] ] ...
    }
    allow none
    banner [disabled | enabled]
    banner-text [string]
    inactivity-timeout [integer]
    include [string]
    login [disabled | enabled]
    log-level [debug | debug1 | debug2 | debug3 | error | fatal |
               info | quiet | verbose]
edit sshd
    all-properties
    non-default-properties
```

Display

```
list sshd
list sshd [option]
show running-config sshd
show running-config sshd [option]
    all-properties
    non-default-properties
    one-line
```

Description

You can use the **sshd** component to configure a secure channel between the BIG-IP system and other devices.

F5 Networks recommends that users of the Configuration utility exit the utility before changes are made to the system using the **sshd** component. This is because making changes to the system using this component causes a restart of the **sshd** daemon. Likewise, restarting the **sshd** daemon creates the necessity for a restart of the Configuration utility.

Examples

modify sshd allow add {192.168.0.0/255.255.0.0}

Creates an initial range of IP addresses (**192.168.0.0** with a netmask of **255.255.0.0**) that are allowed to log in to the system.

modify sshd allow add {192.168.1.245}

Adds the IP address, **192.168.1.245**, to the existing list of IP addresses that are allowed to log in to the system.

modify sshd login enabled

Enables SSH login to the system.

modify sshd inactivity-timeout 3600

Sets an inactivity timeout of **60** minutes for SSH logins to the system.

modify sshd log-level error

Sets the sshd message log level to ERROR.

modify sshd banner enabled banner-text "NOTICE: Improper use of this computer may result in prosecution!"

Creates a banner that displays when a user attempts to log in to a system using SSH.

Note that you must enclose the banner text in double quotation marks, and then type single quotation marks outside the double quotation marks. You can also use the backslash character to escape each quotation mark as well as any other special characters that the system might process (for example, exclamation point !).

Options

- **allow**
  Configures servers in the **/etc/hosts.allow** file. The default value is **all**.

WARNING

*Using the value **none** resets the sshd daemon to allow all servers access to the system. F5 Networks recommends that you do not use the value **none** with the **sshd** component.*

- **banner**
  Enables or disables the display of the banner text field when a user logs in to the system using SSH. The default value is **disabled**.
- **banner-text**
  When the **banner** option is enabled, specifies the text to include in the banner that displays when a user attempts to log on to the system.
- **inactivity-timeout**
  Specifies the number of seconds before inactivity causes an SSH session to log out. The default value is **0** (zero) seconds, which indicates that inactivity timeout is disabled.

- **include**
  Warning: Do not use this option without assistance from the F5 Technical Support team. The system does not validate the commands issued using the **include** option. If you use this option incorrectly, you put the functionality of the system at risk.
- **login**
  Enables or disables SSH logins to the system. The default value is **enabled**.
- **log-level**
  Specifies the minimum sshd message level to include in the system log. The possible values are:
  - **debug - debug3**
    Indicates that the minimum sshd message level that the system logs is the specified debugging level of messages.
  - **error**
    Indicates that the minimum sshd message level that the system logs is error.
  - **fatal**
    Indicates that the minimum sshd message level that the system logs is fatal.
  - **info**
    Indicates that the minimum sshd message level that the system logs is informational.
  - **quiet**
    Indicates that the system does not log sshd messages.
  - **verbose**
    Indicates that the system logs all sshd messages.

See Also

edit, *list*, *modify*, *show*, *tmsh*

state-mirroring

Configures connection mirroring for a BIG-IP® system that is part of a redundant pair in a high availability system.

Syntax

Configure the **state-mirroring** component within the **sys** module using the syntax in the following sections.

Modify

```
modify state-mirroring
    addr [IP address]
    peer-addr [IP address]
    secondary-addr [IP address]
    secondary-peer-addr [IP address]
    state [enabled | disabled]
edit state-mirroring
    all-properties
    non-default-properties
```

Display

```
list state-mirroring
list state-mirroring [option]
show running-config state-mirroring
show running-config state-mirroring [option]
    all-properties
    non-default-properties
    one-line
```

Description

You can use this component to configure connection mirroring on a system that is part of a redundant pair in a high availability system.

Connection mirroring is the process of duplicating connections from the active system to the standby system. Enabling this setting ensures a higher level of connection reliability, but it may also have an impact on system performance.

Examples

modify state-mirroring state enabled addr 192.168.10.10 peer-addr 192.168.10.20

Enables and configures connection mirroring for a high availability system in which one BIG-IP system has an IP address of **192.168.10.10**, and its peer has an IP address of **192.168.10.20**.

modify state-mirroring state enabled

Re-enables connection mirroring for a system for which connection mirroring was disabled.

Options

- **addr**
  Specifies the primary self-IP address on this unit to which the peer unit in this redundant pair mirrors its connections. The default value is **::**.
- **peer-addr**
  Specifies the primary self-IP address on the peer unit to which this unit mirrors its connections. The default value is **::**.
- **secondary-addr**
  Specifies another self-IP address on this unit to which the peer unit mirrors its connections when the primary address is unavailable. The default value is **::**.
- **secondary-peer-addr**
  Specifies another self-IP address on the peer unit to which this unit mirrors its connections when the primary peer address is unavailable. The default value is **::**.
- **state**
  Enables or disables connection mirroring. The default value is **enabled**.

See Also

edit, *list*, *modify*, *show*, *tmsh*

sync-sys-files

Syncs a pre-defined set of system files from a device.

Syntax

Sync a pre-defined set of system files within the **sys** module using the syntax shown in the following sections.

Run

```
run sync-sys-files
    from [IP address]
```

Display

```
show sync-sys-files
```

Description

You can use the **sync-sys-files** component to sync system files listed in /usr/share/defaults/sys_file.spec from a remote device. You can run this command only if the **Administrator** user role is assigned to your user account.

Examples

run sync-sys-files from 172.27.34.182

Syncs the list of files (as given in **/usr/share/defaults/sys_file.spec**) from the
IP address **172.27.34.182**.

show sync-sys-files

Shows the last sync time and the source device from where the files are synced.

Options

- **from**
  Specifies the IP address used for configuration synchronization on the device from which you want to sync system files.

syslog

Configures the BIG-IP® system log.

Syntax

Configure the **syslog** component within the **sys** module using the syntax in the following sections.

Modify

```
modify syslog
    auth-priv-from [alert | crit | debug | emerg | err | info |
                    notice | warning]
    auth-priv-to [alert | crit | debug | emerg | err | info |
                  notice | warning]
    cron-from [alert | crit | debug | emerg | err | info |
               notice | warning]
    cron-to [alert | crit | debug | emerg | err | info | notice |
             warning]
    daemon-from [alert | crit | debug | emerg | err | info |
                 notice | warning]
    daemon-to [alert | crit | debug | emerg | err | info | notice |
               warning]
    description [string]
    include [string]
    iso-date [enabled | disabled]
    console-log [enabled | disabled]
    kern-from [alert | crit | debug | emerg | err | info | notice |
               warning]
    kern-to [alert | crit | debug | emerg | err | info | notice |
             warning]
    local6-from [alert | crit | debug | emerg | err | info | notice |
                 warning]
    local6-to [alert | crit | debug | emerg | err | info | notice |
               warning]
    mail-from [alert | crit | debug | emerg | err | info | notice |
               warning]
    mail-to [alert | crit | debug | emerg | err | info | notice |
             warning]
    messages-from [alert | crit | debug | emerg | err | info |
                   notice | warning]
    messages-to [alert | crit | debug | emerg | err | info | notice |
                 warning]
    remote-servers [ add | delete | modify | replace-all-with] {
      [name] {
          host [hostname]
          local-ip [IP address]
          remote-port [port number]
      }
    }
    remote-servers none
    user-log-from [alert | crit | debug | emerg | err | info | notice |
                   warning]
    user-log-to [alert | crit | debug | emerg | err | info | notice |
                 warning]
```

```
edit syslog
    all-properties
    non-default-properties
```

Display

```
list syslog
list syslog [option]
show running-config syslog
show running-config syslog [option]
    all-properties
    non-default-properties
    one-line
```

Description

You can use the **syslog** component to configure the system log.

Examples

modify syslog auth-priv-from warning

Resets the lowest level of messages about user authentication that are included in the system log to messages with a level of warning, error, critical, alert, and emergency.

modify syslog auth-priv-to warning

Resets the highest level of messages about user authentication that are included in the system log to messages with a level of warning, error, critical, alert, and emergency.

Options

- **auth-priv-from**
  Specifies the lowest level of messages about user authentication to include in the system log. The default value is **notice**.
- **auth-priv-to**
  Specifies the highest level of messages about user authentication to include in the system log. The default value is **emerg**.
- **cron-from**
  Specifies the lowest level of messages about time-based scheduling to include in the system log. The default value is **warning**.
- **cron-to**
  Specifies the highest level of messages about time-based scheduling to include in the system log. The default value is **emerg**.
- **daemon-from**
  Specifies the lowest level of messages about daemon performance to include in the system log. The default value is **notice**.

- **daemon-to**
  Specifies the highest level of messages about daemon performance to include in the system log. The default value is **emerg**.
- **description**
  User defined description.
- **host**
  Specifies the IP address of a remote server to which syslog sends messages. The default value is **none**.
- **include**

WARNING

*Do not use this option without assistance from the F5 Technical Support team. The system does not validate the commands issued using the **include** options. If you use this option incorrectly, you put the functionality of the system at risk.*

- **iso-date**Enables or disables the ISO date format for messages in the log files. The default value is **disabled**.

- **console-log**
  Enables or disables logging emergency syslog messages to the console. The default value is **enabled**.
- **kern-from**
  Specifies the lowest level of kernel messages to include in the system log. The default value is **notice**.
- **kern-to**
  Specifies the highest level of kernel messages to include in the system log. The default value is **emerg**.
- **local-ip**
  Specifies the IP address of the interface syslog binds with in order to log messages to a remote host. For example, if you want syslog to log messages to a remote host that is connected to a VLAN, you set this parameter to the self IP address of the VLAN.
- **local6-from**
  Specifies the lowest error level for messages from the local6 facility to include in the log. The default value is **notice**.
- **local6-to**
  Specifies the highest error level for messages from the local6 facility to include in the log. The default value is **emerg**.
- **mail-from**
  Specifies the lowest level of mail log messages to include in the system log. The default value is **notice**.
- **mail-to**
  Specifies the highest level of mail log messages to include in the system log. The default value is **emerg**.

- **messages-from**
  Specifies the lowest level of messages about user authentication to include in the system log. The default value is **notice**.
- **messages-to**
  Specifies the highest level of system messages to include in the system log. The default value is **warning**.
- **remote-port**
  Specifies the port number of a remote server to which syslog sends messages. The default value is **514**.
- **remote-servers**
  Configures the remote servers, identified by IP address, to which syslog sends messages. The default value is **none**.
- **user-log-from**
  Specifies the lowest level of user account messages to include in the system log. The default value is **notice**.
- **user-log-to**
  Specifies the highest level of user account messages to include in the system log. The default value is **emerg**.

See Also

edit, *list*, *modify*, *show*, *tmsh*

tmm-info

Displays information about the Traffic Management Microkernel (tmm) daemon.

Syntax

Display statistics for the **tmm-info** component within the **sys** module using the syntax in the following section.

Display

```
show tmm-info
    (default | exa | gig | kil | meg | peta | raw | tera | yotta | zetta)
    global
```

Description

You can use the **tmm-info** component to display information about the **tmm** daemon. The purpose of this daemon is to direct all application traffic passing through the BIG-IP® system.

Options

For information about the options that you can use with the command **show**, see **help show**.

See Also

show, *tmm-traffic*, *tmsh*

tmm-traffic

Displays Traffic Management Microkernel (tmm) statistics.

Syntax

Configure the **tmm-traffic** component within the **sys** module using the syntax in the following section.

Modify

```
reset-stats tmm-traffic
```

Display

```
show tmm-traffic
    (default | exa | gig | kil | meg | peta | raw | tera | yotta | zetta)
    global
```

Description

You can use the **tmm-traffic** component to display **tmm** traffic statistics, including errors and redirected connections. The purpose of this daemon is to direct all application traffic passing through the BIG-IP® system.

Options

For information about the options that you can use with the command **show**, see **help show**.

For information about the options that you can use with the command **reset-stats**, see **help reset-stats**.

See Also

reset-stats, *show*, *tmm-info*, *traffic*, *tmsh*

traffic

Displays or resets traffic statistics for the system.

Syntax

Configure the **traffic** component within the **sys** module using the syntax in the following section.

Modify

```
reset-stats traffic
```

Display

```
show traffic
    (default | exa | gig | kil | meg | peta | raw | tera | yotta | zetta)
```

Description

You can use the **traffic** component to display traffic statistics, including for client, server, Packet Velocity® ASIC (PVA), miscellaneous, and authorization traffic. You can also reset the traffic statistics to zero at any time.

Options

For information about the options that you can use with the command **show**, see **help show**.

For information about the options that you can use with the command **reset-stats**, see **help reset-stats**.

See Also

reset-stats, *show*, *pva-traffic*, *tmm-info*, *tmm-traffic*, *tmsh*

ucs

Loads or saves a UCS (.ucs) file.

Syntax

Configure the **ucs** component within the **sys** module using the syntax in the following sections.

Modify

```
save ucs [file name]
    no-private-key
    passphrase
load ucs [file name]
    include-chassis-level-config
    no-license
    no-platform-check
    passphrase
    reset-trust
delete ucs [ file name ]
```

Display

```
list ucs
show ucs [file name]
```

Description

You can use the **ucs** component to save the running configuration of the system into a UCS file. Additionally, you can modify the running configuration of the system by loading an existing UCS file.

When you save a UCS file, the file is saved to the default directory, /var/local/ucs.

When you load a UCS file in shell mode, the system searches for the file using the relative path to the default directory (/var/local/ucs). When you load a UCS file in bash mode, the system searches the current directory first. If the file is not found in the current directory, the default directory is then searched.

Examples

save ucs myucs

Saves the running configuration of the system into the file **myucs.ucs**.

load ucs myucs

Modifies the running configuration of the system by loading the configuration contained in the **myucs.ucs** file.

delete ucs myucs

Delete **myucs.ucs** in the default directory, /var/local/ucs/.

list ucs

Displays existing UCS files in the default directory, /var/local/ucs/.

Options

- **include-chassis-level-config**
  During restore of the UCS file, include chassis level configuration that is shared among boot volume sets. For example, cluster default configuration.
- **no-private-key**Indicates that the UCS file can be saved without private key information.
- **passphrase**
  Specifies the passphrase that is necessary to load the specified UCS file.
- **no-license**
  Performs a full restore of the UCS file and all the files it contains, with the exception of the license file. The option must be used to restore a UCS on RMA devices (Returned Materials Authorization).
- **no-platform-check**
  Bypasses the platform check and allows a UCS that was created using a different platform to be installed. By default (without this option), a UCS created from a different platform is not allowed to be installed.
- **reset-trust**
  When specified, the device and trust domain certs and keys are not loaded from the UCS. Instead, a new set is regenerated.

See Also

load, *list*, *save*, *show*, *tmsh*

version

Displays software version information for the BIG-IP® system.

Syntax

Display statistics for the **version** component within the **sys** module using the syntax in the following section.

Display

```
show version
    detail
```

Description

You can use the **version** component to display the software version running on the system, including a list of hotfixes that you have applied to the system.

Examples

show version

Displays software version information.

show version detail

Displays more extensive software version information about the system, including the operating system kernel information, and details about each hotfix that you have applied to the system.

Options

For information about the options that you can use with the command **show**, see **help show**.

See Also

show, *tmsh*

90

sys application

- Introducing the sys application module
- Alphabetical list of components

Introducing the sys application module

You can use the tmsh components that reside within the sys application module to manage application templates and services. For more information about the tmsh hierarchical structure, see Chapter 2, *Understanding and Using the Traffic Management Shell*.

Alphabetical list of components

The remainder of this chapter lists the tmsh components that are available in the sys application module.

apl-script

Provides scripts that can be included by an application template.

Syntax

Configure the **apl-script** component within the **sys application** module using the syntax in the following sections.

Edit

```
create apl-script [name]
modify apl-script [name]
  apl-checksum [[string] | none]
  apl-signature [[string] | none]
  description [[string] | none]
  ignore-verification [true | false]
edit apl-script [ [ [name] | [glob] | [regex] ] ... ]
  all-properties
```

Display

```
list apl-script
list apl-script [ [ [name] | [glob] | [regex] ] ... ]
```

Delete

```
delete apl-script [name]
```

Generate

Note

generate cryptographic signature or checksum based on apl script text.

```
generate sys application apl-script [name]
    checksum
    signature
```

Description

An APL script contains APL that can be directly included into application templates. APL scripts provide a convenient way to build libraries of common presentation elements. For detailed description of application presentation language elements, See **help page of sys application template**

Examples

The following is a fairly simple example of an APL script and a template that makes
use of the APL script. The APL script defines a user type that can then be used
multiple times in different templates.

```
sys application apl-script com.f5.apl.example {
    define string port validator "PortNumber"
}
sys application template example_template {
    actions {
        definition {
            presentation {
                include "com.f5.apl.example"
                section my_section {
                    string address1
                    port portnum1
                    string address2
                    port portnum2
                }
            }
        }
    }
}
```

generate my_script checksum

Generate a checksum for the script text and add the checksum as a property.

generate my_script signature signing-key my_key

Generate a signature for the script text using the specified private key
and add the signature as a property.

Note: For a script which includes a checksum or signature to succesfully load,
the script text contents must match the stored checksum or signature.

To temporarily stop the verification of signature or checksum and still retain the checksum or
signature, the **ignore-verification** attribute must be set to **true**. This is done by editing the script and adding the **ignore-verification** attribute.

To completely clear the signature or checksum, simply set the attribute **script-signature** or
script-checksum to empty string "". By doing so, the script will be processed as if it was
never signed or checksumed.

```
modify apl-script my_script {
   description none
   script {
   }
   ignore-verification true
   script-checksum 74778e7b13016e0b9329a17f8d2da601
   total-signing-status checksum
   verification-status checksum-verified
}
```

Options

You can use these options with the **apl-script** command:

- **checksum**
  Generate a checksum for the script text and add the checksum to the script as a property. Only for use with the **generate** command.
- **description**
  User defined description.
- **glob**
  Displays the items that match the **glob** expression. See **help glob** for a description of **glob** expression syntax.
- **name**
  Specifies a unique name for the component. This option is required for the commands **create** and **modify**.
- **regex**
  Displays the items that match the regular expression. The regular expression must be preceded by an at sign (@[regular expression]) to indicate that the identifier is a regular expression. See **help regex** for a description of regular expression syntax.
- **script**
  Contains the APL text that can be imported into application templates.
- **signature**
  Generate a signature for the script text using the specified private key and add the signature to the script as a property. Only for use with the **generate** command.
- **signing-key**
  The private key to use for signing the script. Only for use with the **signature** option.

See Also

create, *delete*, *edit*, glob, *list*, *modify*, regex, *template* and *generate*.

custom-stat

Provides derived statistics for iStats.

Syntax

Configure the **custom-stat** component within the **sys application** module using the syntax in the following sections.

Edit

```
create custom-stat [key]
modify custom-stat [key]
   app-service [[string] | none]
   keyspace [string]
   formula [string]
   measure [string]
edit custom-stat [ [ [key] | [glob] | [regex] ] ... ]
  all-properties
```

Display

```
list custom-stat
list custom-stat [ [ [key] | [glob] | [regex] ] ... ]
```

Delete

```
delete custom-stat [key]
```

Description

Statistics are derived for objects in the given keyspace based on the given formula, producing the given measure.

Examples

create sys application custom-stat myKey
keyspace sys.application.service
measure conns_per_min
formula "rate counter conns 60"

Creates a derived iStat.

Options

You can use these options with the **custom-stat** component:

- **app-service**
  Specifies the name of the application service to which the object belongs. The default value is **none**. **Note:** If the **strict-updates** option is **enabled** on the application service that owns the object, you cannot modify or delete the object. Only the application service can modify or delete the object.
- **formula**
  Specifies the first token in the formula indicates the computation to be made. Currently only rates are supported.

  ```
  rate <source_measure_type> <source_measure_name>
       <rate_window_in_seconds>
  ```

  rate computes the rate of change of the source measure over the last <rate_window_in_seconds> seconds. This is applicable only to numeric measures. The derived measure is of type **gauge**.
- **keyspace**
  Specifies that a derived iStat will be computed for all objects in the given keyspace for which the formula is computable (the source measure of the correct type exists).
- **measure**
  Specifies the name of the derived measure to be created. The type of the derived measure is dependent on the formula.

See Also

create, *modify*, *service*

service

Configures traffic management application services.

Syntax

Modify the **service** component within the **sys application** module using the syntax shown in the following sections.

Create/Modify

```
create service [name]
modify service [name]
  description [string]
  device-group [[string] | default | non-default | none]
  execute-action [name]
  lists [add | delete | modify | replace-all-with] {
     [name] {
        value { [string]... }
        value none
        encrypted [yes | no]
     }
  }
  lists none
  strict-updates [disabled | enabled]
  tables [add | delete | modify | replace-all-with] {
     [name] {
        column-names { [name] ... }
        encrypted-columns { [name] ... }
        rows { { row { [value] ... } row { [value] ... } ... } }
        rows none
     }
  }
  tables none
  template [name]
  traffic-group [[string] | default | non-default | none]
  variables [add | delete | modify | replace-all-with] {
     [name] {
        value [string]
        encrypted [yes | no]
     }
  }
  variables none
metadata
  [add | delete | modify] {
    [metadata_name ... ] {
      value [ "value content" ]
      persist [ true | false ]
    }
}
edit service [ [ [name] | [glob] | [regex] ] ... ]
    all-properties
    non-default-properties
```

Display

```
list service
list service [ [ [name] | [glob] | [regex] ] ... ]
show running-config service
show running-config service [ [ [name] | [glob] | [regex] ] ... ]
  all-properties
  non-default-properties
  one-line
  partition
```

Delete

```
delete service [name]
```

Options

You can use these options with the **service** component:

- **description**
  User defined description.
- **device-group**
  Specifies the name of the device group to which the application service is assigned. If this property is modified with the **default** keyword, the value of the parent folder or partition will be used and the **inherited-devicegroup** property will be set to true.
- **execute-action**
  Runs the specified template action associated with the service.
- **glob**
  Displays the items that match the **glob** expression. See **help glob** for a description of **glob** expression syntax.
- **lists**
  Provides the set of list variables and values that are passed to template scripts.
- **metadata**
  Associates user defined data, each of which has name and value pair and persistence. The default value is **persistent**, which means the data will be saved into the config file.
- **regex**
  Displays the items that match the regular expression. The regular expression must be preceded by an at sign (@[regular expression]) to indicate that the identifier is a regular expression. See **help regex** for a description of regular expression syntax.
- **strict-updates**
  Specifies whether configuration objects contained in the application service can be directly modified outside the context of the system's application service management interfaces.
- **tables**
  Provides the set of table variables and values that are passed to template scripts.

- **template**
  The template defines the configuration for the application service. Generic application service has no template associated with it. This can be changed after the service has been created to move the service to a new template. A templated application service can be converted to a generic application service by setting new template to none or empty string. Similarly a generic application service can be made templated by associating it with the existing template.
- **template-modified**
  Indicates that the application template used to deploy the service has been modified. The application service should be updated to make use of the latest changes.
- **template-prerequisite-errors**
  Indicates any missing prerequisites associated with the template that defines this application.
- **traffic-group**
  The name of the traffic group that the application service is assigned to. If this property is modified with the "default" keyword, the value of the parent folder or partition will be used and the **inherited-trafficgroup** property will be set to true.
- **variables**
  The set of atomic variables and values that are passed to template scripts.

See Also

create, *delete*, *edit*, glob, *list*, *modify*, regex, *tmsh*

template

Enables the creation of user-defined templates.

Syntax

Configure the **template** component within the **sys application** module using the syntax in the following sections.

Create/Edit/Modify

```
create template [name]
modify template [name]
  actions [add | delete | modify | replace-all-with] {
     definition {
        html-help [string]
        implementation { [string] }
        presentation  { [string] }
        role-acl [add | delete | modify | replace-all-with] {
            [role]
        }
        role-acl none
        run-as [string]
     }
  }
  description [string]
  requires-modules [add | delete | modify | replace-all-with] {
      [string]
  }
  requires-bigip-version-max [string]
  requires-bigip-version-min [string]
  metadata
    [add | delete | modify] {
      [metadata_name ... ] {
        value [ "value content" ]
        persist [ true | false ]
      }
  }
edit template [name]
```

Display

```
list template
list template [name]
```

Delete

```
delete template [name]
```

Generate

Note

generate cryptographic signature or checksum based on template fields - html-help, implemenation, macro and presentation in definition section.

```
generate template [name]
    checksum
    signature
```

Save/Load

```
save template [name] file [filename]
load template [filename]
```

Description

Application templates allow a user to define a custom interface for easily creating complex configurations. The user can create multiple templates for various types of configurations. Once built, the user can use a template to create an application, which is a specific set of configuration objects (such as Virtual IP addresses, pools, and so forth), that work together to perform some task.

The template is composed of two primary parts, the presentation and the implementation.

The presentation section describes a form (a set of questions and user interface elements) that the user must fill out in order to create an application.

The implementation section describes how the values collected from the user (the form variables) are used to generate the actual configuration objects which are part of the application.

The presentation section of the template is written in a simple language called Application Presentation Language or APL. The implementation section of the template is written in TCL and provides access to tmsh scripting commands.

Application Lifecycle

Before describing in detail how a template is written, it is important to explain how the resulting template will be used. Since templates are used to create and edit applications, it makes sense to review the application lifecycle.

Application Creation

The user selects which template to use for his application. The system presents an empty form, based on the template's presentation script that the user fills out and submits. The system collects and stores the form variables in a newly created application object. Configuration objects are generated based on the form variables by the template's implementation script.

Application Editing

The user selects an existing application that he would like to change. The system reloads the form associated with the template that was used to create the application and refills all form variables using the previous user input, which is gathered from the application object. The user edits the form and submits it. The template's implementation script is run again to compute a new set of configuration objects for the application. The system alters the current configuration objects associated with the application to match the newly computed set of configuration objects, including creating, modifying, and deleting objects as needed.

Application Deletion

The user selects an application to delete. All configuration objects associated with the application are removed.

Application Template Language

The application template language describes the user interface presented to a user making a new application, or editing an existing application. It describes what questions to ask, how the questions are presented (for example, a free form field or a list of options), and the names of the variables used to store the values the user inputs.

It consists of a set of primitive form elements (string, choice, etc), a set of grouping and organization constructs (section, table, etc), methods for hiding or displaying portions of the form based on the values of other portions (optional), a method to associate human-readable text with various form elements (text) and methods for creating user defined types(define group, define section, etc) for reuse of application presentation language elements.

Primitive Elements

Primitive elements represent the actual user interface components. The system displays each primitive element as part of the form, and associates it with a form variable. The following lists the basic primitive types:

- **choice**
  A list of options from which the user can select (a drop-down menu).
  choice <var-name> [default "<def value>"] [display "<def value>"] {"<choice1>", "<choice2>", ...}

- **editchoice**
  Multiple choices are available that the user can select, or a new value can be entered if the choices are not acceptable.
  choice <var-name> [default "<def value>"] [display "<def value>"] {"<choice1>", "<choice2>", ...}

- **multichoice**
  Similar to a basic choice element except that multiple items may be selected from the available choices.
  choice <var-name> [default "<def value>"] [display "<def value>"] {"<choice1>", "<choice2>", ...}

- **password**
  Similar to a string element except the contents may be obscured to prevent others from seeing the value.
  password <var-name> [default "<def value>"] [display "<def value>"] [required]

- **string**
  A basic text box into which the user can enter an arbitrary string.
  string <var-name> [default "<def value>"] [display "<def value>"] [required] [validator "<validator name>"]

Each primitive element is associated with a variable name, which defines where the value collected by the form is stored. In addition, primitive elements can have additional parameters such as a default value, a validation method that provides for additional requirements (for example, the string must be an IP address).

The following defines the format for the string primitive values, using normal BNF syntax:

- **default** - A sensible default value to which the string is initialized when a new application is created.

- **display** - Directs the renderer how to display the element. This can be **small**, **medium**, **large**, **xlarge**, or **xxlarge**.

- **required** - If present, a valid value must be entered before the application can be created.

- **validator** - The name of a well known validation method.

Section

The section construct is used to group form variables (primitives) into logical sections for display.

Each section is named, and header text can be defined for a section using the text construct.

Every variable must be inside a section. The format for a section is:

```
section <section-name> { <contents...> }
```

For example, to represent the data associated with a virtual IP:

```
section vip
{
   string address
   string port default "80" display "small"
}
```

Table

The table construct is similar to section, except that it represents a grouping of elements that can be repeated zero or more times. The syntax for table and section are identical.

```
table <list-name> { <contents...> }
```

For example, to collect a list of nodes from a user to populate a pool, you can add any number of nodes, each of which has an address and port:

```
section pool
{
  table members
  {
    string address
    string port default "80" display "small"
  }
}
```

The table above is displayed using a JavaScript-editing widget that enables you to add and remove pool members. Each member contains two form variables: **address** and **port**.

Optional

The optional construct allows the form elements to be hidden or shown based on the state of other form elements. The syntax of the optional construct is:

```
optional (<expr>) { <contents...> }
```

The expression in the optional construct is evaluated during the display of the form. The content section is displayed or hidden, based on its value.

To dynamically hide parts of the presentation based on the answer to a earlier question, use the variable name in the expression:

```
section chooseopts {
  choice show_section_1 {"yes", "no"}
}
section section1
{
  optional (chooseopts.show_section_1 == "yes")
```

```
  {
    string str
  }
}
```

User Defined Types

The define construct allows the creation of user-defined types out of primitive types. The defined type can then be used multiple times independently at different places. This is especially useful in conjunction with the include element because types can be defined in the included application presentation language script and then used where necessary in the template. For more details on application presentation language script, See **help sys application apl-script**.

For example, user defined choice type can be defined as below and can be reused at multiple sections:

```
define choice yesno {
  "Yes", "No"
}
section ssl_section {
    yesno use_ssl
}
section optimizations {
    yesno use_wa
    yesno offload_ssl
}
```

The define group construct allows the creation of user-defined type to allow the user to group multiple elements of existing types together. The defined type can be reused multiple times independently similar to the above.

For example IpAddress and port can be grouped into a user-defined type and reused in multiple sections:

```
define group addrport {
   string addr required validator "IpAddress"
   string port
}
section http_section {
   addrport server
}
section sip_section {
   addrport client
   addrport server
}
```

Localization

The text element lets you define the localized text labels for sections, table, row and other sub-elements. For message element, body text can be localized in addition to the label. Similarly for the choice, editchoice and multichoice element, display text associated with each choice value can be localized. The syntax for the text element is:

```
text ["<locale>"] {
  <section var_name> "<label>"
  <section var_name>.<string or password var_name> "<label>"
  <section var_name>.<message var_name> "<label>" "<body>"
```

```
  <section var_name>.<choice, editchoice or multichoice var_name> "<label>" {
"<display text1>" => "<choice1>", "<display text2>" => "<choice2>", ... }
}
```

Depending on the locale used (setting in the browser), particular text label, body text or choice display text will be shown to the user.

For example, string, message and choice display texts can be localized as below.

```
section http
{
  message intro
  string address
  string port default "80" display "small"
  choice pools default "pool1" { "pool1", "pool2", "pool3" }
  choice profile default "http" tcl {
      set choices "no
          append choices "http
          append choices [tmsh::run_proc f5.app_utils:get_items ltm profile http]
          return $choices
  }
}
```

```
text {
  vs "HTTP Application"
  vs.intro "Introduction" "This template supports simple web server implementations"
  vs.address "What IP address do you want to use for this virtual server?"
  vs.port "What port do you want to use for this virtual server?"
  vs.pools "Use pool.." {"Internal" => "pool1", "Public cloud" => "pool2", "Private
data center" => "pool3" }
  vs.profile "Use profile.."  { "Do not use profile" => "no", "Use F5's recommended
profile" => "http" }
}
```

```
text "de_AU" {
  vs "HTTP-Anwendung"
  vs.intro "Einfuhrung "Diese vorlage unterstutzt einfache
web-server-implementierungen"
  vs.address "Welche ip-adresse mochten Sie fur diesen virtuellen Server zu
verwenden?"
  vs.port "Welchen port willst du fur diesen virtuellen Server zu verwenden?"
  vs.pools "Verwenden pool.." {"intern" => "pool1", "Privat Rechenzentrum" => "pool3",
"Offentliche Cloud" => "pool2" }
  vs.profile "Mit profil.."  { "Verwenden sie kein profil" => "no", "Verwenden von F5
empfohlen profil" => "http" }
}
```

A user from Austria will see the german text, all other locales will see the default (locale-less) text.

While localizing choice value display text, users are allowed to use different ordering of choice values in each locale. If TCL is used to populate the choices, then best effort is made to match what is returned in the TCL to the given localized choice value. In the above example, the embedded TCL script for profile will return two static choices (no and http) followed by the list of all http profiles. These static choices are localized, but not the other results. When the TCL results contain a mix of localized and non-localized choices, the localized choices will always be listed first in the order specified in the text element.

With the localization, message body and static choices will become optional in the declaration. If the message body is provided in both the declaration and in text element, the body in the text element will override the body in the variable declaration. Same applicable for the display text of choice value provided in declaration. The recommended syntax for choice, editchoice and multichoice element is to give just the choice values in the variable declaration, and give the display text of the choices in the text element.

Tmsh Scripting Support

Once the user finishes editing an application, the form variables are saved, and the implementation section of the associated template is run. The implementation section is an ordinary TCL script and can use the standard set of **tmsh** scripting extensions. In addition, there are a few template-specific additions.

First, access to the form variable is done using the syntax, where **<section >** is the name of the section to which the variable belongs, and **<name >** is the name of the form variable:

```
$::<section>__<name>
```

Next, a table can be iterated over, and for each list element, the components of the list can be gathered using the **tmsh::get_field_value command**. For example, for the pool member example described in the section regarding the list, you can use the following syntax:

```
foreach member $::pool__members {
  set the_addr [tmsh::get_field_value $member address]
  set the_port [tmsh::get_field_value $member port]
  # Do something with the_addr and the_port
}
```

This means for variable access can also be used within a script macro. Expansion of a macro is done using the **tmsh::expand_macro** command. Usage:

```
tmsh::expand_macro [macro] [name_value_pair_list]
```

The variables defined in the presentation are automatically available from within the macro. If additional variables are needed from within the macro, they can be specified via **name_value_pair_list**. Variables defined this way will take precendence over duplicate variables defined in the presentation.

Tmsh Built-In Variables

Specific details on application and application template is provided to implementation section using built-in variables. Following are the variables available for use.

- **tmsh::app_name**
  Stores the user-provided application name string.
- **tmsh::app_name_path**
  Stores the path name of application in configuration database.

- **tmsh::app_template_name**
  Stores the user-provided application template name including the path in configuration database.
- **tmsh::app_template_action**
  Stores the application template action name.

Examples

The following template example shows both the presentation and implementation sections. (It lacks some features, such as use of optional, defaults, validators, etc.)

```
presentation {
  section basic
  {
    choice ssl_enabled { "true", "false" }
    string addr
    string more_stuff
    table servers
    {
      string addr
      string port
      string ratio
    }
  }
  text
  {
     basic "Some example questions"
     basic.ssl_enabled "Should SSL be enabled?"
     basic.addr "What address should we use for the VIP?"
     basic.servers.addr "Address"
     basic.servers.port "Port"
  }
}
implementation {
  if { $::basic__ssl_enabled }
  {
    set profile_name [format "%s_%s" $tmsh::app_name clientssl]
    tmsh::create ltm profile client-ssl $profile_name
    append profile_name " http"
set destination "$::basic__addr:https"
set monitor https
   }
   else
   {
set profile_name http
set destination "$::basic__addr:http"
set monitor http
   }
set pool_name [format "%s_%s" $tmsh::app_name pool]
set members {
  foreach server $::basic__servers {
    append members [tmsh::get_field_value $server addr]
    append members ":"
    append members [tmsh::get_field_value $server port]
    append members " { ratio "
    append members [tmsh::get_field_value $server ratio]
```

```
    append members "}"
    append members " "
}
append members }

tmsh::create ltm pool $pool_name \
  members replace-all-with $members \
  monitor $monitor

set vs_name [format "%s_%s" $tmsh::app_name virtual]
tmsh::create ltm virtual $vs_name \
  destination $destination \
  profiles replace-all-with "{ $profile_name }" \
  snat automap \
  pool $pool_name \
  http-class none
 }
```

generate my_app checksum

Generate a checksum for the template definition and add the checksum as a property.

generate my_app signature signing-key my_key

Generate a signature for the template definition using the specified private key
and add the signature as a property.

Note: For a template which includes a checksum or signature to succesfully load,
the definition contents must match the stored checksum or signature.

To temporarily stop the verification of signature or checksum and still retain the checksum or
signature, the **ignore-verification** attribute must be set to **true**. This is done by editing the script and adding the **ignore-verification** attribute.

To completely clear the signature or checksum, simply set the attribute **script-signature** or
script-checksum to empty string "". By doing so, the script will be processed as if it was
never signed or checksumed.

```
sys application template my_tmpl {
   actions {
      definition {
         html-help {
            <!-- insert html help text -->
         }
         implementation {
            # insert tmsh script
         }
         presentation {
            # insert apl script
         }
         role-acl none
         run-as none
      }
   }
   description "This is my template"
```

```
    ignore-verification true
    script-checksum 74778e7b13016e0b9329a17f8d2da601
    total-signing-status checksum
    verification-status checksum-verified
}
```

Options

- **actions**
  Adds, deletes, or replaces a set of template actions. You can configure the following options for an action:
  - **html-help**
    The help for the application template action formatted as HTML.
  - **implementation**
    The script that is run to create the configuration objects associated with the application.
  - **name**
    The name of the application template action.
  - **presentation**
    The questions that must be answered to create an application from the template.
  - **role-acl**
    The list of roles that are allowed to run the action.
  - **run-as**
    The user account that will be used to run the implementation script. If no account is specified, the script is run as the calling user.
  - **checksum**
    Generate a checksum for the template definition and add the checksum to the template as a property. Only for use with the **generate** command.
  - **signature**
    Generate a signature for the template definition using the specified private key and add the signature to the template as a property. Only for use with the **generate** command.
  - **signing-key**
    The private key to use for signing the template. Only for use with the **signature** option.
- **description**
  User defined description.
- **metadata**
  Associates user defined data, each of which has name and value pair and persistence. The default value is **persistent**, which saves the data into the config file.
- **partition**
  Displays the administrative partition within which the application template resides.

- **prerequisite-errors**
  A message indicating if there are any errors with the prerequisites for the template on the current BIG-IP system. If there are errors no applications can be created from this template. If there are no errors then the template is valid.
- **requires-modules**
  Adds, deletes, or replaces the list of modules that are required to be provisioned for this template to work.
- **requires-bigip-version-max**
  Specifies the maximum version of BIG-IP software required by this template.
- **requires-bigip-version-min**
  Specifies the minimum version of BIG-IP software required by this template.

Third Party Tcl Library Usage

A selection of third party libraries have been tested to work within the CLI script environment. These include MD5, BASE64, SHA1/SHA256, HTTP, TLS, TCL Perl, LDAP client, and XML parser. The TCL packages can only reside in the **/use/share/tcl8.4** directory.

Important

Only these tested packages are supported currently.

The following example shows how the Tcl package command can make use of the XML parser:

```
cli script /Common/use_xml {

proc script::EStart {tag attlist args} {
  array set attr $attlist
    puts "Element "$tag" started with [array size attr] attributes"
}

proc script::PCData text {
  incr ::count [string length $text]
}

proc script::run {} {
  namespace eval :: {
    set count 0
  }
  puts "running use_xml...
  set pkg_name xml
  if {[catch {package require $pkg_name 3.2}]} {
    puts "No package found: $pkg_name!
  }
  else {
    puts "Found package: $pkg_name!
    set parser [xml::parser]
    $parser configure -elementstartcommand script::EStart -characterdatacommand
script::PCData
    set fp [open "/shared/test.xml" r]
    set text [read $fp]
```

```
    $parser parse $text
    puts "The document contains $::count characters"
    close $fp
  }
}
```

Here are some additional examples:

```
cli script /Common/use_sha1 {
proc script::run {} {
  set pkg_name sha1
  if {[catch {package require $pkg_name}]} {
    puts "No package found: $pkg_name!
  }
  else {
    puts "Found package: $pkg_name!
    puts "TCL does SHA1 now:"
    puts [sha1::sha1 -hex "TCL does SHA1"]
  }
}

cli script /Common/use_base64 {
proc script::run {} {
  set pkg_name base64
  if {[catch {package require $pkg_name}]} {
    puts "No package found: $pkg_name!
  }
  else {
    puts "Found package: $pkg_name!
    set chemical [encoding convertto utf-8 "Cu2088Hu2081u2080Nu2084Ou2082"]
    set encoded [base64::encode $chemical]
    set caffeine [encoding convertfrom utf-8 [base64::decode $encoded]]
    puts "Caffeine: $caffeine"
  }
}
```

See Also

edit, *list*, *modify*, *show*, *tmsh*, *generate*

91

sys crypto

- Introducing the sys crypto module
- Alphabetical list of components

Introducing the sys crypto module

You can use the tmsh components that reside within the sys crypto module to manage cryptographic objects in the system. For more information about the tmsh hierarchical structure, see Chapter 2, *Understanding and Using the Traffic Management Shell*.

Alphabetical list of components

The remainder of this chapter lists the tmsh components that are available in the sys crypto module.

cert

Manage cryptographic certificates on the BIG-IP® system.

Syntax

Manage cryptographic **cert** s using the syntax in the following section.

Create

```
create cert [name]
    city [string]
    common-name [string]
    consumer
      [enterprise-manager | iquery | iquery-big3d | ltm | webserver]
    country [string]
    email-address [string]
    key [string]
    lifetime [days]
    organization [string]
    ou [string]
    state [string]
    subject-alternative-name [string]
```

Install

```
install cert [name]
    consumer
      [enterprise-manager | iquery | iquery-big3d | ltm | webserver]
    from-editor
    from-local-file [filename]
    from-url [URL]
    no-overwrite
```

Delete

```
delete cert [name]
```

Description

You can use the **cert** component to create, install, and delete cryptographic certificates, and bundles.

Examples

create cert example key testkey.key common-name "My Company Inc." country "US"

Generates a self signed certificate named "example.crt". A key with the specified name "testkey.key" in this case must be installed on the system in order for this operation to succeed. The cert extension (".crt") will be appended to the created cert name if it is not already provided in the name.

create cert /myfolder/example key testkey.key common-name "My Company Inc." country "US"

Similar to above, but creates the cert "example.crt" in the folder "/myfolder" instead of the default "/Common". The specified folder "/myfolder" must already exist in order for this operation to succeed.

create cert server2 key server2.key common-name "My Company Inc." country "US" consumer webserver

Generates a self-signed certificate named server2.crt. The consumer attribute, "webserver", is used to cause the files to be placed directly in the path which can be found by the BIG-IP system httpd. A pre-existing key named "server2.key" must exist in the web server's key path in order for this operation to succeed. Please note that for non LTM consumer's key and cert names must be the same.

install cert example from-editor

Opens an interactive editor session into which can be pasted a certificate for import into the BIG-IP system. A certificate file-object will be created with the name example which contains the contents saved from the editor session.

install cert example from-local-file /tmp/example.crt

Obtains a certificate from the file located at /tmp/example.crt.

install cert example from-url http://example.com/example.crt

Obtains a certificate from a remote host, based on the URI specified.

delete cert example.crt

Deletes the certificate "example.crt" from the system.

Options

- **city**
  Specifies the x509 city field to be used in creation of the certificate.
- **common-name**
  Specifies the x509 common-name to be used in creation of the certificate.
- **consumer**
  Specifies the system component by which a certificate will be consumed. The default behavior is to create file-objects for use by ltm components. This is the same as specifying "ltm" for this property. If a component other than "ltm" is specified then files will be installed/created in locations where the specified components can find them. For example, for component "webserver", certificates will be placed in the webservers ssl directories.

- **country**
  Specifies the x509 country to be used in creation of the certificate. The country must be a 2 letter country code.
- **email-address**
  Specifies the x509 email-address to be used in creation of the certificate.
- **from-editor**
  Specifies that the certificate should be obtained from a text editor session. This allows certificates to be imported via cut-n-paste from another location as long as they are in a text representation.
- **from-local-file**
  Specifies a local file path from which a certificate is to be copied.
- **from-url**
  Specifies a URI which is to be used to obtain a certificate for import into the system.
  The URL syntax is protocol dependent. Supported schemes are "HTTP", "HTTPS", "FTP", "FTPS" & "FILE."
- **no-overwrite**
  Specifies option of not overwriting a certificate if it is in the scope.
- **key**
  Specifies a **key** from which a certificate should be generated when using the create command.
- **organization**
  Specifies the x509 organization to be used in creation of the certificate.
- **ou**
  Specifies the x509 organizational unit to be used in creation of the certificate.
- **state**
  Specifies the x509 state or province of the certificate.
- **subject-alternative-name**
  Specifies standard X.509 extensions as shown in RFC 2459. Allowed values e.g. DNS:example.com, IP:192.168.1.1, IP:12:34, email:user@example.com, URI:http://www.example.com

See Also

create, *install*, *delete*, *tmsh*

check-cert

Examines certificates and displays or logs any that have expired on the BIG-IP® system.

Syntax

Run a check on the expiration date of LTM certificates, in the **sys crypto** module by using the syntax below.

Run

```
run check-cert [certificate-file-name]
    log [enabled | disabled]
    stdout [enabled | disabled]
    verbose [enabled | disabled]
```

Description

You can use the **check-cert** command to check the expiration date of certificate(s) and print the results to the screen and/or log them to /var/log/ltm.

Options

- **log**
  Specifies whether results should be logged or not. By default they will be logged.
- **stdout**
  Specifies whether results should be printed to STDOUT or not. By default they will be printed.
- **verbose**
  Specifies whether verbose output should be emitted or not, such as information about all certificates being checked rather than just those which return unfavorable results. By default verbose output is disabled.

Examples

run check-cert

Checks all certificate file-objects known by MCPD, and displays information about any certificates which have expired or which are close to expiration. By default this information is printed to the screen and logged to /var/log/ltm.

run check-cert default.crt

Runs the check on the specific certificate "default.crt"

run check-cert verbose

Displays expiration information about all certificates, not just those that have expired or have impending expirations.

run check-cert log disabled

Prints the results to screen but does not log them.

run check-cert stdout disabled

Logs the results to /var/log/ltm, but does not print them to the screen.

See Also

run, *tmsh*

client

Manage remote crypto clients.

Syntax

Manage crypto **client** s using the syntax in the following section.

Create/Modify

```
create client [name]
modify client [name]
    addr [ip address]
    connection-reset
    heartbeat [integer]
    max-retries [integer | infinite]
    port [integer]
    profiles [add | delete | replace-all-with] { [profile_name ...] }
    profiles [none]
    req-timeout [integer]
    retry-interval [integer]
```

Display

```
list client
list client [ [ [name] | [globl] | [regex] ] ... ]
```

Delete

```
delete client [name]
```

Description

You can use the **client** component to manage remote crypto clients.

Examples

create client example addr 10.1.1.1 port 12100 profiles add { serverssl tcp }

Creates a remote crypto client named "example" that will use a remote crypto
server with the IP address "10.1.1.1" on port "12100". The remote crypto client
will use SSL over a TCP connection to communicate with the remote crypto server.

Options

- **addr**
  Specifies the IP address of the remote crypto server.
- **connection-reset**
  Resets the connection to the remote crypto server.
- **heartbeat**
  Specifies the number of seconds to wait before sending a heartbeat request. A value of 0 disables the sending of heartbeat requests. The default value is **30** seconds.
- **max-retries**
  Specifies the maximum number of times to retry connecting to the remote crypto server.
  If the maximum retries value is infinite, the crypto client retries connecting until a connection is made.
  The default value is **infinite**.
- **port**
  Specifies the port used by the remote crypto server.
- **profiles**
  Specifies a list of profiles that the remote crypto client will use to communicate with remote the remote crypto server.
- **req-timeout**
  Specifies the timeout in milliseconds for crypto requests to complete. The default value is **5000** milliseconds.
- **retry-interval**
  Specifies the interval in seconds between attempts to connect to the remote crypto server. The default value is **10** seconds.

See Also

create, *delete*, glob, *list*, *modify*, regex, *tmsh*

crl

Manage certificate revocation lists on the BIG-IP® system.

Syntax

Manage **crl** s using the syntax in the following section.

Install

```
install crl [name]
    ca-file [filename]
    consumer
      [enterprise-manager | iquery | iquery-big3d | ltm | webserver]
    from-editor
    from-local-file [filename]
    from-url [URL]
```

Delete

delete crl [name]

Description

You can use the **crl** component to install, and delete certificate revocation lists. The file-objects created by these operations can be used in other BIG-IP system configuration blocks such as ssl profiles.

Examples

install crl example from-editor

Opens an interactive editor session into which can be pasted a crl for import into the BIG-IP system. A crl file-object will be created with the name example which contains the contents saved from the editor session.

install crl example from-local-file /tmp/example.crl

Obtains a crl from the file located at /tmp/example.crl and installs it as example.crl. The crl extension (".crl") will be appended to the installed crl name if it is not already provided in the name.

install crl /myfolder/myexample from-local-file /tmp/example.crl

Similar to above, but installs the crl "myexample.crl" in folder "/myfolder" instead of the default "/Common". The specified folder "/myfolder" must already exist in order for this operation to succeed.

install crl example from-url http://example.com/example.crl

Obtains a crl from a remote host, based on the URI specified.

delete crl example.crl

Deletes the certificate revocation list "example.crl" from the system.

Options

- **consumer**
  Specifies the system component by which the certificate revocation list will be consumed. The default behavior is to create file-objects for use by ltm components. This is the same as specifying "ltm" for this property. If a component other than "ltm" is specified then files will be installed/created into locations where the specified components can find them. For example, for component "webserver", crls will be placed in the webservers ssl directories.
- **from-editor**
  Specifies that the crl should be obtained from a text editor session. This allows crls to be imported via cut-n-paste from another location as long as they are in a text representation.
- **from-local-file**
  Specifies a local file path from which the crl is to be copied.
- **from-url**
  Specifies a URI which is to be used to obtain the crl for import into the configuration of the system.
  The URL syntax is protocol dependent. Supported schemes are "HTTP", "HTTPS", "FTP", "FTPS" & "FILE."

See Also

create, *install*, *delete*, *tmsh*

key

Manage cryptographic keys and related objects on the BIG-IP® system.

Syntax

Manage cryptographic **key** s and related objects of the **sys crypto** module using the syntax in the following section.

Create

```
create key [name]
   challenge-password [string]
   city [string]
   common-name [string]
   consumer
     [enterprise-manager | iquery | iquery-big3d | ltm | webserver]
   country [string]
   curve-name [prime256v1 | secp384r1]
   email-address [string]
   key-size [512 | 1024 | 2048 | 4096]
   key-type [dsa-private | ec-private | rsa-private]
   lifetime [days]
   organization [string]
   ou [string]
   passphrase [passphrase]
   prompt-for-password
   security-type [fips | normal | password | nethsm]
   state [string]
   subject-alternative-name [string]
```

Install

```
install key [name]
    consumer
      [enterprise-manager | iquery | iquery-big3d | ltm | webserver]
    from-editor
    from-local-file [filename]
    from-url [URL]
    no-overwrite
```

Delete

```
delete key [name]
```

Description

You can use the **key** component to create, install, and delete cryptographic keys, and associated cryptographic objects. The file-objects created by these operations can be used in other BigIP configuration blocks such as ssl profiles.

Examples

create key mykey

Generates a 2048-bit (default-sized) RSA key file object named "mykey.key". The appropriate extension will be added to the generated key/cert if not already a part of the provided name.

create key /myfolder/mykey

Similar to above, but creates the key "mykey.key" in folder "/myfolder" instead of the default "/Common". The specified folder "/myfolder" must already exist in order for this operation to succeed.

create key example gen-cert gen-csr common-name "My Company Inc." country "US"

Generates a 2048-bit (default-sized) RSA key file object named "example.key" and a self signed certificate named "example.crt". Also, a certificate signing request will be printed to the console for use in obtaining a signed certificate from a certificate authority if desired.

create key my gen-cert gen-csr prompt-for-password common-name "My Company Inc." country "US"

Similar to above, creates key "my.key" but also prompts for a password to be used as a challenge password in the certificate authority signing procedure.

create key server2 gen-cert gen-csr common-name "My Company Inc." country "US" consumer webserver

Generates a key and self signed certificate identified by server2. The consumer attribute, "webserver", is used to cause these files to be placed directly in the paths which can be found by the BigIP's httpd.

install key example from-editor

Opens an interactive editor session into which can be pasted a key for import into the BigIP system. A key file-object will be created with the name example which contains the contents saved from the editor session.

install key example from-local-file /tmp/example.key

Obtains a key from the file located at /tmp/example.key.

install key example from-url http://example.com/my.key

Obtains a key from a remote host, based on the URI specified.

delete key example.key

Deletes the key "example.key" from the system.

Options

- **challenge-password**
  Specifies the challenge password to create the certificate request key.
- **city**
  Specifies the x509 city field to be used in creation of the certificate associated with the given key.

- **common-name**
  Specifies the x509 common-name to be used in creation of the certificate associated with the given key.
- **consumer**
  Specifies the system component by which a key and/or associated cryptographic file will be consumed. The default behavior is to create file-objects for use by ltm components. This is the same as specifying "ltm" for this property. If a component other than "ltm" is specified then files will be installed/created into locations where the specified components can find them. For example, for component "webserver", keys and certs will be placed in the webservers ssl directories.
- **country**
  Specifies the x509 country to be used in creation of the certificate associated with the given key. The country must be a 2 letter country code.
- **curve-name**
  Specifies the curve name to be used in creation of elliptc curve (EC) key. This options applies only when generating EC keys. Default value is **prime256v1**.
- **email-address**
  Specifies the x509 email-address to be used in creation of the certificate associated with the given key.
- **from-editor**
  Specifies that the key should be obtained from a text editor session. This allows keys to be imported via cut-n-paste from another location as long as they are in a text representation.
- **from-local-file**
  Specifies a local file path from which a key is to be copied.
- **from-url**
  Specifies a URI which is to be used to obtain a key for import into the configuration of the system.
  The URL syntax is protocol dependent. Supported schemes are "HTTP", "HTTPS", "FTP", "FTPS" & "FILE."
- **no-overwrite**
  Specifies option of not overwriting a key if it is in the scope.
- **gen-certificate**
  Specifies that in addition to generating a key, a self-signed certificate will also be created. If this option is specified then x509 attributes should also be specified. Minimally, you must also specify a common-name.
- **gen-csr**
  Specifies that a certificate signing request should be generated along with the key. The CSR will be displayed to the terminal for the purposes of use in getting a certificate signed by an outside authority. X509 attributes must also be specified.
- **key-size**
  Specifies the size, in bits, of the key to be generated. This option does not apply when generating EC keys.

- **key-type**
  Specifies the type of cryptographic key to be generated.
- **lifetime**
  Specifies the certificate life time to be used in creation of the certificate associated with the given key.
- **organization**
  Specifies the x509 organization to be used in creation of the certificate associated with the given key.
- **ou**
  Specifies the x509 organizational unit to be used in creation of the certificate associated with the given key.
- **prompt-for-password**
  Specifies that a password should be prompted for and then used as a challenge password in generation of the CSR (Certificate Signing Request).
- **security-type**
  Specifies the level of security used in storing the key in question. For example a security-type of FIPS means that the key should be stored on a FIPS card if one is available.
- **state**
  Specifies the x509 state or province of the certificate associated with the given key.
- **passphrase**
  Specifies an optional passphrase with which the key has been protected. It may be used by consumers of the key in the data-plane or control-plane to decrypt it.
- **subject-alternative-name**
  Specifies standard X.509 extensions as shown in RFC 2459. Allowed values e.g. DNS:example.com, IP:192.168.1.1, IP:12:34, email:user@example.com, URI:http://www.example.com

See Also

create, *install*, *delete*, *tmsh*

master-key

Displays the configuration of the master key for the BIG-IP® system.

Syntax

Display the configuration of the **master-key** component within the **sys crypto** module using the syntax in the following section.

Display

```
show master-key
    field-fmt
```

Modify

```
modify master-key
    prompt-for-password
```

Run

```
run master-key diagnostic
```

Description

You can use the **master-key** command to manipulate the system master key. Users with the Administrator role or the Certificate Manager role can set the key to a value of their choosing by using the 'prompt-for-password' option during a modify operation. All other roles, including Resource Administrators, are prohibited from setting the master key.

Use the 'diagnostic' option of the run command to test the key integrity.

Examples

show master-key

Displays, in a table, information about the system's master key.

show master-key field-fmt

Displays, in field format, information about the system's master key.

run master-key diagnostic

Loads the device key. Uses the device key to decrypt the master key file to test the integrity of the keys. On success, there is no output. There will be a response only if there is an error.

modify master-key prompt-for-password

Create a master-key based on a word or phrase of your choosing. You can use this to manually synchronize several devices without having to copy keys between them.

Options

For information about the options that you can use with the command **show**, see **help show**.

See Also

show, *tmsh*

pkcs12

Install pkcs12 keys and certificates on the BIG-IP® system.

Syntax

Install keys and certificates from pkcs12 files using the syntax in the following section.

Install

```
install pkcs12 [name]
    consumer
      [enterprise-manager | iquery | iquery-big3d | ltm | webserver]
    from-local-file [filename]
    from-url [URL]
    key-passphrase
    key-security-type
      [fips | password | normal]
    passphrase [passphrase]
    no-overwrite
```

Description

You can use the **pkcs12** component to install cryptographic keys and certificates from **pkcs12** formatted files. The file-objects created by these operations can be used in other BigIP configuration blocks such as ssl profiles.

Examples

install pkcs12 example from-local-file /tmp/example.p12

Obtains a pkcs12 from the file located at /tmp/example.p12, and installs the key and certificate from that file as file-objects named "example.key" and "example.crt" respectively.

install pkcs12 /myfolder/example from-local-file /tmp/example.p12

Similar to above, but installs the key "example.key" and cert "example.crt" in folder "/myfolder" instead of the default "/Common". The specified folder "/myfolder" must already exist in order for this operation to succeed.

install pkcs12 example prompt-for-password from-local-file /tmp/example.p12

Same as above but also prompts for a password which is to be used to decrypt the **pkcs12** file.

install pkcs12 my from-url http://example.com/my.p12

Obtains a pkcs12 file from a remote host, based on the URL specified.

install pkcs12 server consumer webserver from-local-file /tmp/example.p12

Obtains a pkcs12 file from /tmp/example.p12 and installs the key and certificate from that file as file-objects that can be used by the "webserver". The consumer attribute, "webserver", is used to cause these files to be placed directly in the paths which can be found by the BigIP's httpd.

Options

- **consumer**
  Specifies the system component by which a key and associated certificate from a PKCS12 file will be consumed. The default behavior is to create file-objects for use by ltm components. This is the same as specifying "ltm" for this property. If a component other than "ltm" is specified then files will be installed/created into locations where the specified components can find them. For example, for component "webserver", keys and certs will be placed in the webservers ssl directories.
- **from-local-file**
  Specifies a local file path from which the contents of the PKCS12 are to be read.
- **from-url**
  Specifies a URI which is to be used to obtain a PKCS12 for import into the configuration of the system.
  The URL syntax is protocol dependent. Supported schemes are "HTTP", "HTTPS", "FTP", "FTPS" & "FILE."
- **key-passphrase**
  Specifies the passphrase to be used to encrypt the key.
- **key-security-type**
  Specifies the security type of the key. Default is set to "normal".
- **passphrase**
  Specifies the passphrase to be used to decrypt the PKCS12 file.
- **no-overwrite**
  Specifies option of not overwriting key/certificate if they are in the scope.

See Also

install, *tmsh*

server

Manage remote crypto servers.

Syntax

Manage crypto **server** s using the syntax in the following section.

Create/Modify

```
create server [name]
modify server [name]
    addr [ip address]
    clients [add | delete | replace-all-with] { [ip_addr/prefixlen ...] }
    clients [none]
    port [integer]
    profiles [add | delete | replace-all-with] { [profile_name ...] }
    profiles [none]
```

Display

```
list server
list server [ [ [name] | [globl] | [regex] ] ... ]
```

Delete

```
delete server [name]
```

Description

You can use the **server** component to manage remote crypto servers.

Examples

create server example addr 10.1.1.1 port 12100 profiles add { clientssl tcp }

Creates a remote crypto server named "example" that will listen for remote crypto clients on IP address "10.1.1.1" and port "12100". The remote crypto server will use SSL over a TCP connection to communicate with remote crypto
clients.

Options

- **addr**
  Specifies the IP address of the remote crypto server.

- **clients**
  Specifies a list of allowed client IP addresses and subnets. An empty list allows all clients.
- **port**
  Specifies the port used by the remote crypto server.
- **profiles**
  Specifies a list of profiles that the remote crypto server will use to communicate with remote crypto clients.

See Also

create, *delete*, glob, *list*, *modify*, regex, *tmsh*

92

sys crypto fips

- Introducing the sys crypto fips module
- Alphabetical list of components

Introducing the sys crypto fips module

You can use the tmsh components that reside within the sys crypto fips module to manage components of the fips140 subsystem, when applicable. For more information about the tmsh hierarchical structure, see Chapter 2, *Understanding and Using the Traffic Management Shell*.

Alphabetical list of components

The remainder of this chapter lists the tmsh components that are available in the sys crypto fips module.

by-handle

Manipulates FIPS 140 keys by-handle

Syntax

Manipulate FIPS 140 keys **by-handle** within the **sys crypto fips** module using the syntax in the following section.

Delete

```
delete by-handle [handle]
```

Description

You can use the **by-handle** component to manage the FIPS 140 keys by-handle.

You can determine the handle of a FIPS 140 key using the following command:

show sys crypto fips

Examples

delete by-handle 101

Deletes a FIPS 140 key given by the handle **101**.

Options

For information about the options that you can use with the **delete** command, see **help delete**.

See Also

show, *tmsh*

external-hsm

Configures parameters for external HSM FIPS hardware.

Description

You can use the **external-hsm** command to set parameters about the HSM vendor name and the password to login to the external HSM hardware.

Syntax

Configures FIPS **external-hsm** within the **sys crypto fips** module using the syntax in the following section.

Create

```
create external-hsm
modify external-hsm vendor [thales | safenet | none]
modify external-hsm password [password]
modify external-hsm num-threads [no. of threads]
```

Display

```
list external-hsm
list external-hsm vendor
list external-hsm password
list external-hsm num-threads
```

Delete

```
delete external-hsm
```

key

Displays information about FIPS keys

Syntax

Display information about **key** component within the **sys crypto fips** module using the syntax in the following section.

Display

```
show key [label]
    field-fmt
    all-properties
    include-public-keys
```

Description

You can use the **key** command to view information about private and public keys contained in the FIPS hardware.

Examples

show key

Displays the list of all private keys stored in the FIPS hardware and their meta-data.

show key example

Displays information specifically about the FIPS private key(s) which match the label "example".

show key field-fmt

Displays, in field format, information about private keys stored in the FIPS hardware.

show key all-properties

Displays all information about the FIPS contained private keys, including: **handle**, a numerical value used by the FIPS hardware to identify individual keys; **modulus-length**, the cryptographic modulus length of the key; and **modulus**, the modulus associated with the key, displayed as a string of hex octets separated by colons.

show key include-public-keys

Displays the list of all private and public keys stored in the FIPS hardware and their meta-data. Note that public keys are not displayed by default and need not exist for normal operation of FIPS hardware.

Options

include-public-keys

Specifies that public keys should be selected for output in addition to private.

For information about the options that you can use with the command **show**, see **help show**.

See Also

show, *tmsh*

93

sys daemon-log-settings

- Introducing the sys daemon-log-settings module
- Alphabetical list of components

Introducing the sys daemon-log-settings module

You can use the tmsh components that reside within the sys daemon-log-settings module to configure the BIG-IP® system settings and display information about the system. For more information about the tmsh hierarchical structure, see Chapter 2, *Understanding and Using the Traffic Management Shell*.

Alphabetical list of components

The remainder of this chapter lists the tmsh components that are available in the sys daemon-log-settings module.

clusterd

Changes the log-level of or displays information about the daemon **clusterd**.

Syntax

Configure the **clusterd** component within the **sys daemon-log-settings** module using the syntax in the following sections.

Modify

```
modify clusterd
    log-level [critical | debug | error | informational | notice |
               warning]
edit clusterd
    all-properties
    non-default-properties
```

Display

```
list clusterd
    all-properties
    non-default-properties
    one-line
```

Description

You can use the **clusterd** component to change the level of the messages about the **clusterd** daemon that appear in the system logs. Additionally, you can display information about the daemon.

Examples

list clusterd

Displays information about the **clusterd** daemon.

modify clusterd log-level critical

Changes the level of the messages about the **clusterd** daemon that display in the system log to **critical**.

Options

- **log-level**
  Specifies the level of log messages for the specified daemon that you want to display in the system log.

See Also

edit, *list*, *modify*, *tmsh*

csyncd

Changes the log-level of or displays information about the daemon **csyncd**.

Syntax

Configure the **csyncd** component within the **sys daemon-log-settings** module using the syntax in the following sections.

Modify

```
modify csyncd
    log-level [critical | debug | error | informational | notice |
               warning]
edit csyncd
    all-properties
    non-default-properties
```

Display

```
list csyncd
    all-properties
    non-default-properties
    one-line
```

Description

You can use the **csyncd** component to change the level of the messages about the **csyncd** daemon that appear in the system logs. Additionally, you can display information about the daemon.

Examples

list csyncd

Displays information about the **csyncd** daemon.

modify csyncd log-level critical

Changes the level of the messages about the **csyncd** daemon that display in the system log to **critical**.

Options

- **log-level**
  Specifies the level of log messages for the specified daemon that you want to display in the system log.

See Also

edit, *list*, *modify*, *tmsh*

icrd

Changes or displays the audit level of the daemon **icrd**.

Syntax

Configure the **icrd** component within the **sys daemon-log-settings** module using the syntax in the following sections.

Modify

```
modify icrd
    audit [ none | modifications | all ]
edit icrd
    all-properties
    non-default-properties
```

Display

```
list ind
    all-properties
    non-default-properties
    one-line
```

Description

You can use the **icrd** component to change the audit level of the **icrd** daemon.

Examples

list icrd

Displays audit log level of the **icrd** daemon.

modify icrd audit all

Changes the audit level of the **icrd** daemon to **all**. This means that all commands executed by the icrd daemon get audited

Options

- **audit**
  Specifies the audit level of log messages for the icrd daemon in the audit logs.

See Also

edit, *list*, *modify*, *tmsh*

lind

Changes the log-level of or displays information about the daemon **lind**.

Syntax

Configure the **lind** component within the **sys daemon-log-settings** module using the syntax in the following sections.

Modify

```
modify lind
    log-level [critical | debug | error | informational | notice |
            warning]
edit lind
    all-properties
    non-default-properties
```

Display

```
list lind
    all-properties
    non-default-properties
    one-line
```

Description

You can use the **lind** component to change the level of the messages about the **lind** daemon that appear in the system logs. Additionally, you can display information about the daemon.

Examples

list lind

Displays information about the **lind** daemon.

modify lind log-level critical

Changes the level of the messages about the **lind** daemon that display in the system log to **critical**.

Options

- **log-level**
  Specifies the level of log messages for the specified daemon that you want to display in the system log.

See Also

edit, *list*, *modify*, *tmsh*

mcpd

Changes the log-level of or displays information about the daemon **mcpd**.

Syntax

Configure the **mcpd** component within the **sys daemon-log-settings** module using the syntax in the following sections.

Modify

```
modify mcpd
    audit [all | disabled | enabled | verbose]
    log-level [alert | critical | debug | emergency | error |
               informational | notice | panic | warning]
edit mcpd
    all-properties
    non-default-properties
```

Display

```
list mcpd
    all-properties
    non-default-properties
    one-line
```

Description

You can use the **mcpd** component to change the level of the messages about the **mcpd** daemon that appear in the system logs. Additionally, you can display information about the daemon.

Examples

list mcpd

Displays information about the **mcpd** daemon.

modify mcpd log-level critical

Changes the level of the messages about the **mcpd** daemon that display in the system log to **critical**.

Options

- **audit**
  Enables or disables auditing for the mcpd daemon, and specifies verbose or all as the auditing level. The default is **disabled**.

- **log-level**
  Specifies the level of log messages for the specified daemon that you want to display in the system log.

See Also

edit, *list*, *modify*, *tmsh*

tmm

Changes the log-level of or displays information about the Traffic Management Microkernel (**tmm**).

Syntax

Configure the **tmm** component within the **sys daemon-log-settings** module using the syntax in the following sections.

Modify

```
modify tmm
    arp-log-level [debug | error | informational | notice |
      warning]
    http-compression-log-level [debug | error | informational |
      notice | warning]
    http-log-level [debug | error | informational |
      notice | warning]
    ip-log-level [debug | informational | notice | warning]
    irule-log-level [debug | error | informational |
      notice | warning]
    layer4-log-level [debug | informational | notice]
    net-log-level [critical | debug | error | informational |
      notice | warning]
    os-log-level [alert | critical | debug | emergency |
      error | informational | notice | warning]
    pva-log-level [debug | informational | notice]
    ssl-log-level [alert | critical | debug | emergency |
      error | informational | notice | warning]
edit tmm
    all-properties
    non-default-properties
```

Display

```
list tmm
    all-properties
    non-default-properties
    one-line
```

Description

You can use the **tmm** component to change the level of the messages about the **tmm** that appear in the system logs. Additionally, you can display information about the **tmm**.

Examples

list tmm

Displays information about the **tmm**.

modify tmm http-compression-log-level critical

Changes the level of the messages about HTTP compression that display in the system log to **warning**.

Options

- **arp-log-level**
  Specifies the lowest level of ARP messages from the **tmm** daemon to include in the system log. The default value is **warning**.
- **http-compression-log-level**
  Specifies the lowest level of HTTP compression messages from the **tmm** daemon to include in the system log. The default value is **error**.
- **http-log-level**
  Specifies the lowest level of HTTP messages from the daemon to include in the system log. The default value is **error**.
- **ip-log-level**
  Specifies the lowest level of IP address messages from the **tmm** daemon to include in the system log. The default value is **warning**.
- **irule-log-level**
  Specifies the lowest level of iRule messages from the **tmm** daemon to include in the system log. The default value is **warning**.
- **layer4-log-level**
  Specifies the lowest level of Layer 4 messages from the **tmm** daemon to include in the system log. The default value is **notice**.
- **net-log-level**
  Specifies the lowest level of network messages from the **tmm** daemon to include in the system log. The default value is **warning**.
- **os-log-level**
  Specifies the lowest level of operating system messages from the **tmm** daemon to include in the system log. The default value is **notice**.
- **pva-log-level**
  Specifies the lowest level of PVA messages from the **tmm** daemon to include in the system log. The default value is **informational**.
- **ssl-log-level**
  Specifies the lowest level of SSL messages from the **tmm** daemon to include in the system log. The default value is **warning**.

See Also

edit, *list*, *modify*, *tmsh*

94

sys disk

- Introducing the sys disk module
- Alphabetical list of components

Introducing the sys disk module

You can use the tmsh components that reside within the sys disk module to configure the BIG-IP® system settings, and display information about the system. For more information about the tmsh hierarchical structure, see Chapter 2, *Understanding and Using the Traffic Management Shell*.

Alphabetical list of components

The remainder of this chapter lists the tmsh components that are available in the sys disk module.

application-volume

Configures an application volume instance.

Syntax

Configure the **application-volume** component in the **sys disk** module using the syntax shown in the following sections.

Display

```
show application-volume [name]
list application-volume [name]
```

Delete

```
delete application-volume [name]
```

Description

The **application-volume** component provides better granularity for managing disks. Physical disks can now be shared by several **application-volumes**. An **application-volume** is physically confined to one logical disk. The visibility of the **application-volume** can be confined to a particular software volume set or it can be global. No **application-volume** properties are allowed to be modified through tmsh or iControl® interfaces.

Examples

delete application-volume mysqldb_MD1.3

Deletes an **application-volume** named **mysqldb_MD1.3**.

show application-volume mysqldb_MD1.3

Displays the configuration details of the **application-volume mysqldb_MD1.3** in a table.

Option

- **logical-disk [name]**
  Specifies the name of the logical disk in which the **application-volume** will be created.
- **owner [unassigned/datastor/mysql/vcmp]**
  Specifies the owner for which this **application-volume** is assigned. unassigned - is the default option and means the volume is not in use and nobody owns it.

- **preservability [discardable/precious]**
  Specifies the if **application-volume** can be discarded by software (for example, during module provisioning). discardable - is the default option.
- **resizeable [false/true]**
  Specifies the if **application-volume** can potentially be resized. false - is the default option.
- **size [integer]**
  Specifies the size of the **application-volume**.
- **volume-set-visibility-restraint [name]**
  Specifies the name of the volume set to which the **application-volume** is constrained, if any.

See Also

delete, *show*, *list*, *tmsh*, *provision*, *logical-disk*

directory

Manages resizing of system directories.

Syntax

Configure the **directory** component in the **sys disk** module using the syntax shown in the following sections.

Modify

```
modify directory [directory_name]
   new-size [new_size]
```

Show

```
show directory
```

Description

The **directory** component assists in resizing system directories. It allows system administrators to increase the size of 4 system directories (/config, /shared, /var, /var/log). This allows more flexible management of the system resources and path for growing the directory sizes on case per case basis.

Examples

modify directory /shared new-size 35000

Increases the size of /shared system directory to 35 MiB.

show directory

Displays a table with currently scheduled directories for resizing. If there are no such directories the output is empty.

See Also

modify, *show*, *tmsh*

logical-disk

Manages logical disks.

Syntax

Configure the **logical-disk** component in the **sys disk** module using the syntax shown in the following sections.

Modify

```
modify logical-disk [name]
vg-reserved [integer]
mode [none/mixed/datastor]
```

Display

```
list logical-disk [name]
```

Description

The **logical-disk** component provides better granularity for managing disks. A physical disk can now be shared by one or more logical disks. A logical disk is physically confined to one physical disk.

Examples

modify logical-disk foo mode mixed vg-reserved 200

Modifies the logical disk **foo** mode property to **mixed** and the **vg-reserved** property size to 200 MiB.

list logical-disk foo

Displays the configuration details of the logical disk named **foo**.

Option

- **mode [none/mixed/datastor/control]**
  Specifies the current mode of the logical disk. The options are:
  - **control** - Indicates that the logical disk is part of a RAID array.
  - **datastor** - Indicates that the entire disk is committed to the datastor module.

- **mixed** - Indicates that the disk contains multiple volumes for software and/or multiple volumes for application data.
- **none** - Indicates that the disk is not in use. This is the default option.

- **size [integer]**
  Specifies the size (MiB) of the logical disk.
- **vg-free [integer]**
  Specifies the usable free space (MiB) available in the logical disk.
- **vg-in-use [integer]**
  Specifies the total logical disk space (MiB) in use.
- **vg-reserved [integer]**
  Specifies the reserved logical disk space (MiB). This space is NOT available for provisioning.

See Also

modify, *list*, *tmsh*, *provision*, *logical-disk*

95

sys file

- Introducing the sys file module
- Alphabetical list of components

Introducing the sys file module

You can use the tmsh components that reside within the sys file module to manage file objects on the system. For more information about the tmsh hierarchical structure, see Chapter 2, *Understanding and Using the Traffic Management Shell*.

Alphabetical list of components

The remainder of this chapter lists the tmsh components that are available in the sys file module.

apache-ssl-cert

Manages an Apache SSL certificate file.

Syntax

Configure the **apache-ssl-cert** component within the **sys file** module using the syntax shown in the following sections.

Create/Modify

```
create apache-ssl-cert [name]
modify apache-ssl-cert [name]
    source-path [URL]
```

Display

```
list apache-ssl-cert
list apache-ssl-cert [ [ [name] | [glob] | [regex] ] ... ]
```

Delete

```
delete apache-ssl-cert [name]
```

Description

You can use the **apache-ssl-cert** component to create, delete, list or modify an SSL certificate.

Examples

create apache-ssl-cert new-cert source-path http:/cert-server/cert_store/certs/cert1.crt

Downloads the certificate from the given URL into file-store, creates an SSL certificate file named **new-cert**, and saves the given URL in the **source-path** attribute.

create apache-ssl-cert new-cert source-path file:/shared/save/cert1.crt

Specifies the location of the file on the local disk (use this when the file has already been created on the local disk).

Supported Url Format

Supported URL schemes are **HTTP**, **HTTPS**, **FTP**, **FTPS**, and **FILE**.

Options

- **bundle-certificates**
  Lists data about all the certificates in the bundle, if the certificate file is a bundle; otherwise, this field will be **none**.
- **certificate-key-size**
  Specifies the number of bits in the key associated with this certificate.
- **checksum**
  Specifies a cryptographic hash or checksum of the file contents for use in verification of file integrity.
- **create-time**
  Specifies the time at which the file-object was created.
- **created-by**
  Specifies the user who originally created the file-object.
- **expiration-date**
  Specifies the date at which this certificate expires. Stored as a POSIX time.
- **expiration-string**
  Specifies a string representation of the expiration date of the certificate.
- **fingerprint**
  Specifies the cryptographic fingerprint of the certificate.
- **is-bundle**
  Specifies whether the certificate file is a bundle (that is, whether it contains more than one certificate).
- **issuer**
  Specifies X509 information of the certificate's issuer. If the cert is a bundle, this displays the issuer information for the primary (first) cert in the bundle.
- **key-type**
  Specifies the type of cryptographic key associated with this certificate.
- **last-update-time**
  Specifies the last time at which the file-object was updated/modified.
- **mode**
  Specifies the UNIX file permissions mode for the file associated with this file-object as a numerical value.
- **revision**
  Identifies the latest revision of the file. The revision starts with 1 and gets incremented on each update.
- **serial-number**
  Specifies the certificate's serial number.
- **size**
  Specifies the size (in bytes) of the file associated with this file object.
- **source-path** [URL]
  This attribute takes a URL, for example:

source-path http://cert-server/cert_store/certs/vs_132.crt

source-path https://cert-server/cert_store/certs/vs_132.crt

source-path ftp://username:password@server/cert_store/certs/vs_132.crt

- **subject**
  Specifies X509 information of the certificate's subject. If the cert is a bundle, this displays the subject information for the primary (first) cert in the bundle.
- **subject-alternative-name**
  Specifies a standard X.509 extension as shown in RFC 2459.
- **updated-by**
  Specifies the user who last updated the file-object.
- **version**
  Specifies the X509 version of the certificate.

See Also

create, *delete*, glob, *list*, *client-ssl*, *server-ssl*, *modify*, regex, *tmsh*

data-group

Manages an external data group file.

Syntax

Manage the **data-group** component within the **sys file** module using the syntax shown in the following sections.

Create/Modify

```
create data-group [name]
modify data-group [name]
    app-service [[string] | none]
    data-group-description [string]
    data-group-name [name]
    separator [string]
    source-path [URL]
    type [integer | ip | string ]
edit data-group [ [ [name] | [glob] | [regex] ] ... ]
```

Display

```
list data-group
list data-group [ [ [name] | [glob] | [regex] ] ... ]
```

Delete

```
delete data-group [name]
```

Description

You can use the **data-group** component to create, edit, delete, list or modify an external data group file.

Examples

create data-group new-dg source-path http:/file-server/data-groups/acl.class type string

Downloads the data-group file from the given URL into file-store, creates an external-data-group file named **new-dg**, and saves the given URL in the source-path attribute.

create data-group new-dg source-path http:/file-server/data-groups/acl.class type string data-group-name dg data-group-description "created for rule xyz"

Downloads the data-group file from the given URL into file-store, creates an external-data-group file named **new-dg**, saves the given URL in the source-path attribute, and creates an **external** data group within the **ltm data-group** module named **dg** with the given description.

create data-group new-dg source-path file:/shared/save/Test.cls type ip

Specifies the location of the file on the local disk (use this when the file has already been created on the local disk).

Supported Url Format

Supported URL schemes are **HTTP**, **HTTPS**, **FTP**, **FTPS**, and **FILE**.

Options

- **app-service**
  Specifies the name of the application service to which the object belongs. The default value is **none**. **Note:** If the **strict-updates** option is **enabled** on the application service that owns the object, you cannot modify or delete the object. Only the application service can modify or delete the object.
- **checksum**
  Specifies a cryptographic hash or checksum of the file contents for use in verification of file integrity.
- **created-by**
  Specifies the user who originally created the file-object.
- **create-time**
  Specifies the time at which the file-object was created.
- **data-group-description**
  Specifies the description of the **external** data group that will be created within the **ltm data-group** module and reference the given data group file. This is optional in the **create** command.
- **data-group-name**
  Specifies the name of the **external** data group that will be created within the **ltm data-group** module and reference the given data group file. This is optional in the **create** command.
- **last-update-time**
  Specifies the last time at which the file-object was updated/modified.
- **mode**
  Specifies the UNIX file permissions mode for the file associated with this file-object as a numerical value.
- **revision**
  The latest revision of the file. The revision starts with 1 and gets incremented on each update.
- **separator**
  Specifies a separator to use when defining the data group. The default value is **:=**.

- **size**
  Specifies the size (in bytes) of the file associated with this file object.
- **source-path** [URL]
  This attribute takes a URL, for example:

source-path http://file-server/data-groups/AUL_1.cls

source-path https://file-server/data-groups/CNN.x

source-path ftp://username:password@server/data-groups/latest.class

source-path file:/shared/save/Test.dat

- **type**
  Specifies the kind of data in the group. This option is required by the **create** command.
  Possible values for type are:
  - **integer**
  - **ip**
  - **string**
- **updated-by**
  Specifies the user who last updated the file-object.

See Also

create, *delete*, *edit*, glob, *list*, *external*, *modify*, regex, *tmsh*

external-monitor

Manages an external monitor file.

Syntax

Manage the **external-monitor** component within the **sys file** module using the syntax shown in the following sections.

Create/Modify

```
create external-monitor [name]
modify external-monitor [name]
    app-service [[string] | none]
    source-path [URL]
edit external-monitor [ [ [name] | [glob] | [regex] ] ... ]
```

Display

```
list external-monitor
list external-monitor [ [ [name] | [glob] | [regex] ] ... ]
```

Delete

```
delete external-monitor [name]
```

Description

You can use the **external-monitor** component to create, edit, delete, list or modify an external-monitor file.

Examples

create external-monitor new-mon source-path http:/file-server/external-monitors/mon_app1

Downloads the monitor file from the given URL into file-store, creates an external-monitor file named **new-mon**, and saves the given URL in the source-path attribute.

create external-monitor new-mon source-path file:/shared/save/Test.mon

Specifies the location of the file on the local disk (use this when the file has already been created on the local disk).

Supported Url Format

Supported URL schemes are **HTTP**, **HTTPS**, **FTP**, **FTPS**, and **FILE**.

Options

- **app-service**
  Specifies the name of the application service to which the object belongs. The default value is **none**. **Note:** If the **strict-updates** option is **enabled** on the application service that owns the object, you cannot modify or delete the object. Only the application service can modify or delete the object.
- **checksum**
  Specifies a cryptographic hash or checksum of the file contents for use in verification of file integrity.
- **created-by**
  Specifies the user who originally created the file-object.
- **create-time**
  Specifies the time at which the file-object was created.
- **last-update-time**
  Specifies the last time at which the file-object was updated/modified.
- **mode**
  Specifies the UNIX file permissions mode for the file associated with this file-object as a numerical value.
- **revision**
  The latest revision of the file. The revision starts with 1 and gets incremented on each update.
- **size**
  Specifies the size (in bytes) of the file associated with this file object.
- **source-path** [URL]
  This attribute takes a URL, for example:

source-path http://file-server/external-monitors/monitor_service

source-path https://file-server/external-monitors/custom_mon.1

source-path ftp://username:password@server/external-monitors/tested.mon

- **updated-by**
  Specifies the user who last updated the file-object.

See Also

create, *delete*, *edit*, glob, *list*, *external*, *modify*, regex, *tmsh*

ifile

Manages an iFile file.

Syntax

Manage the **ifile** component within the **sys file** module using the syntax shown in the following sections.

Create/Modify

```
create ifile [name]
modify ifile [name]
    app-service [[string] | none]
    source-path [URL]
edit ifile [ [ [name] | [glob] | [regex] ] ... ]
```

Display

```
list ifile
list ifile [ [ [name] | [glob] | [regex] ] ... ]
```

Delete

```
delete ifile [name]
```

Description

You can use the **ifile** component to create, edit, delete, list or modify an iFile file.

Examples

create ifile new-ifile source-path http:/tmp/text.txt

Downloads the iFile file from the given URL into file-store and creates an ifile file named **new-ifile**. Saves the given URL in the source-path attribute.

Supported URL schemes are "HTTP", "HTTPS", "FTP", "FTPS" & "FILE"

Options

- **app-service**
  Specifies the name of the application service to which the object belongs. The default value is **none**. **Note:** If the **strict-updates** option is **enabled** on the application service that owns the object, you cannot modify or delete the object. Only the application service can modify or delete the object.

- **checksum**
  A cryptographic hash or checksum of the file contents for use in verification of file integrity.
- **created-by**
  Specifies the user who originally created the file-object.
- **create-time**
  Specifies the time at which the file-object was created.
- **last-update-time**
  Specifies the last time at which the file-object was updated/modified.
- **mode**
  Specifies the UNIX file permissions mode for the file associated with this file-object as a numerical value.
- **revision**
  The latest revision of the file. The revision starts with 1 and gets incremented on each update.
- **size**
  Specifies the size (in bytes) of the file associated with this file object.
- **source-path** [URL]
  This attribute takes a URL, for example:

source-path http://file-server/ifiles/AUL_1.cls

source-path https://file-server/ifiles/CNN.x

source-path ftp://username:password@server/ifiles/latest.class

- **updated-by**
  Specifies the user who last updated the file-object.

See Also

create, *delete*, *edit*, glob, *list*, *ifile*, *modify*, regex, *tmsh*

rewrite-rule

Manages a HTML content rewrite rule.

Syntax

Configure the **rewrite-rule** component within the **sys file** module using the syntax shown in the following sections.

Create/Modify

```
create rewrite-rule [name]
modify rewrite-rule [name]
    local-path [URL]
edit rewrite-rule [ [ [name] | [glob] | [regex] ] ... ]
```

Display

```
list rewrite-rule
list rewrite-rule [ [ [name] | [glob] | [regex] ] ... ]
```

Delete

```
delete rewrite-rule [name]
```

Description

You can use the **rewrite-rule** component to create, edit, delete, list or modify a HTML content rewrite rule.

Examples

create rewrite-rule new-rule local-path /shared/tmp/my_rewrite_rule

Creates a new HTML content rewrite rule using file located by **local-path** and saves path in the **local-path** attribute.

Options

- **checksum**
  Specifies a cryptographic hash or checksum of the file contents for use in verification of file integrity.
- **created-by**
  Specifies the user who originally created the file-object.
- **create-time**
  Specifies the time at which the file-object was created.

- **last-update-time**
  Specifies the last time at which the file-object was updated/modified.
- **mode**
  Specifies the UNIX file permissions mode for the file associated with this file-object as a numerical value.
- **revision**
  Specifies the latest revision of the file. The revision starts with 1 and gets incremented on each update.
- **size**
  Specifies the size (in bytes) of the file associated with this file object.
- **local-path** [path]
  This attribute takes a path, for example:

local-path /shared/tmp/my_rewrite_rule

- **updated-by**
  Specifies the user who last updated the file-object.

See Also

create, *delete*, *edit*, glob, *list*, *html*, *modify*, regex, *tmsh*

ssl-cert

Manages a SSL certificate file.

Syntax

Configure the **ssl-cert** component within the **sys file** module using the syntax shown in the following sections.

Create/Modify

```
create ssl-cert [name]
modify ssl-cert [name]
    app-service [[string] | none]
    source-path [URL]
edit ssl-cert [ [ [name] | [glob] | [regex] ] ... ]
```

Display

```
list ssl-cert
list ssl-cert [ [ [name] | [glob] | [regex] ] ... ]
```

Delete

```
delete ssl-cert [name]
```

Description

You can use the **ssl-cert** component to create, edit, delete, list or modify an SSL certificate.

Examples

create ssl-cert new-cert source-path http:/cert-server/cert_store/certs/cert1.crt

Downloads the certificate from the given URL into file-store, creates an SSL certificate file named **new-cert**, and saves the given URL in the source-path attribute.

create ssl-cert new-cert source-path file:/shared/save/cert1.crt

Specifies the location of the file on the local disk (use this when the file has already been created on the local disk).

Supported Url Format

Supported URL schemes are **HTTP**, **HTTPS**, **FTP**, **FTPS**, and **FILE**.

Options

- **app-service**
  Specifies the name of the application service to which the object belongs. The default value is **none**. **Note:** If the **strict-updates** option is **enabled** on the application service that owns the object, you cannot modify or delete the object. Only the application service can modify or delete the object.
- **bundle-certificates**
  Specifies a list of data about all the certificates in the bundle, if the certificate file is a bundle; otherwise, this field will be none.
- **certificate-key-size**
  Specifies the number of bits in the key associated with this certificate.
- **checksum**
  Specifies a cryptographic hash or checksum of the file contents for use in verification of file integrity.
- **create-time**
  Specifies the time at which the file-object was created.
- **created-by**
  Specifies the user who originally created the file-object.
- **expiration-date**
  Specifies the date at which this certificate expires. Stored as a POSIX time.
- **expiration-string**
  Specifies a string representation of the expiration date of the certificate.
- **fingerprint**
  Specifies the cryptographic fingerprint of the certificate.
- **is-bundle**
  Specifies whether the certificate file is a bundle (that is, whether it contains more than one certificate).
- **issuer**
  Specifies X509 information of the certificate's issuer. If the cert is a bundle, this displays the issuer information for the primary (first) cert in the bundle.
- **key-type**
  Specifies the type of cryptographic key associated with this certificate.
- **last-update-time**
  Specifies the last time at which the file-object was updated/modified.
- **mode**
  Specifies the UNIX file permissions mode for the file associated with this file-object as a numerical value.
- **revision**
  Specifies the latest revision of the file. The revision starts with 1 and gets incremented on each update.
- **serial-number**
  Specifies the certificate's serial number.

- **size**
  Specifies the size (in bytes) of the file associated with this file object.
- **source-path** [URL]
  This attribute takes a URL, for example:

source-path http://cert-server/cert_store/certs/vs_132.crt

source-path https://cert-server/cert_store/certs/vs_132.crt

source-path ftp://username:password@server/cert_store/certs/vs_132.crt

- **subject**
  Specifies X509 information of the certificate's subject. If the cert is a bundle, this displays the subject information for the primary (first) cert in the bundle.
- **subject-alternative-name**
  Specifies a standard X.509 extension as shown in RFC 2459.
- **updated-by**
  Specifies the user who last updated the file-object.
- **version**
  Specifies the X509 version of the certificate.

See Also

create, *delete*, *edit*, glob, *list*, *client-ssl*, *server-ssl*, *modify*, regex, *tmsh*

ssl-crl

Manages a SSL CRL file.

Syntax

Configure the **ssl-crl** component within the **sys file** module using the syntax shown in the following sections.

Create/Modify

```
create ssl-crl [name]
modify ssl-crl [name]
    app-service [[string] | none]
    source-path [URL]
edit ssl-crl [ [ [name] | [glob] | [regex] ] ... ]
```

Display

```
list ssl-crl
list ssl-crl [ [ [name] | [glob] | [regex] ] ... ]
```

Delete

```
delete ssl-crl [name]
```

Description

You can use the **ssl-crl** component to create, edit, delete, list or modify an SSL CRL file.

Examples

create ssl-crl new-crl source-path http:/cert-server/cert_store/CRLs/latest.crl

Downloads the CRL file from the given URL into file-store, creates an SSL CRL file named **new-crl**, and saves the given URL in the source-path attribute.

create ssl-crl new-crl source-path file:/shared/save/copy_10.crl

Specifies the location of the file on the local disk (use this when the file has already been created on the local disk).

Supported Url Format

Supported URL schemes are **HTTP**, **HTTPS**, **FTP**, **FTPS**, and **FILE**.

Options

- **app-service**
  Specifies the name of the application service to which the object belongs. The default value is **none**. **Note:** If the **strict-updates** option is **enabled** on the application service that owns the object, you cannot modify or delete the object. Only the application service can modify or delete the object.
- **checksum**
  Specifies a cryptographic hash or checksum of the file contents for use in verification of file integrity.
- **created-by**
  Specifies the user who originally created the file-object.
- **create-time**
  Specifies the time at which the file-object was created.
- **last-update-time**
  Specifies the last time at which the file-object was updated/modified.
- **mode**
  Specifies the UNIX file permissions mode for the file associated with this file-object as a numerical value.
- **revision**
  Specifies the latest revision of the file. The revision starts with 1 and gets incremented on each update.
- **size**
  Specifies the size (in bytes) of the file associated with this file object.
- **source-path** [URL]
  This attribute takes a URL, for example:

source-path http://cert-server/cert_store/CRLs/backup_10.crl

source-path https://cert-server/cert_store/CRLs/jan_2010.crl

source-path ftp://username:password@server/cert_store/CRLs/latest.crl

- **updated-by**
  Specifies the user who last updated the file-object.

See Also

create, *delete*, *edit*, glob, *list*, *client-ssl*, *server-ssl*, *modify*, regex, *tmsh*

ssl-key

Manages a SSL certificate key file.

Syntax

Configure the **ssl-key** component within the **sys file** module using the syntax shown in the following sections.

Create/Modify

```
create ssl-key [name]
modify ssl-key [name]
    app-service [[string] | none]
    source-path [URL]
    passphrase [passphrase]
edit ssl-key [ [ [name] | [glob] | [regex] ] ... ]
```

Display

```
list ssl-key
list ssl-key [ [ [name] | [glob] | [regex] ] ... ]
```

Delete

```
delete ssl-key [name]
```

Description

You can use the **ssl-key** component to create, edit, delete, list or modify an SSL certificate key file.

Examples

create ssl-key new-key source-path http:/cert-server/cert_store/certs/cert1.key

Downloads the certificate-key file from the given URL into file-store and creates an SSL certficate key file named **new-key**. Saves the given URL in the source-path attribute.

create ssl-key new-key source-path file:/shared/save/cert1.key

Specifies the location of the file on the local disk. Use this when the file has already been created on the local disk.

Supported Url Format

Supported URL schemes are **HTTP**, **HTTPS**, **FTP**, **FTPS**, and **FILE**.

Options

- **app-service**
  Specifies the name of the application service to which the object belongs. The default value is **none**. **Note:** If the **strict-updates** option is **enabled** on the application service that owns the object, you cannot modify or delete the object. Only the application service can modify or delete the object.
- **checksum**
  A cryptographic hash or checksum of the file contents for use in verification of file integrity.
- **create-time**
  Specifies the time at which the file-object was created.
- **created-by**
  Specifies the user who originally created the file-object.
- **key-size**
  Specifies the size of the cryptographic key associated with this file object, in bits.
- **key-type**
  Specifies the cryptographic type of the key in question. That is, which algorithm this key is compatible with.
  The options are:
  - **rsa-private**
    The key is an RSA private key.
  - **dsa-private**
    The key is a DSA based private key.
- **last-update-time**
  Specifies the last time at which the file-object was updated/modified.
- **mode**
  Specifies the UNIX file permissions mode for the file associated with this file-object as a numerical value.
- **passphrase** [passphrase]
  Specifies an optional passphrase with which the key has been protected. It may be used by consumers of the key in the data-plane or control-plane to decrypt it.
- **revision**
  Specifies the latest revision of the file. The revision starts with 1 and gets incremented on each update.
- **security-type**
  Specifies the type of security used to handle or store the key.
  Thie options are:
  - **normal**
    The key resides in a standard form on the file-system. This is the default value.
  - **fips**
    The key is protected by a FIPS device on the system and is only applicable to devices with FIPS support.

  - **password**
    Specifies that the key is protected by a passphrase and stored in encrypted form.
  - **nethsm**
    The key is protected by a FIPS device outside the system.
- **size**
  Specifies the size (in bytes) of the file associated with this file object.
- **source-path** [URL]
  This attribute takes a URL, for example:

source-path http://cert-server/cert_store/certs/vs_132.key

source-path https://cert-server/cert_store/certs/vs_132.key

source-path ftp://username:password@server/cert_store/certs/vs_132.key

- **updated-by**
  Specifies the user who last updated the file-object.

See Also

create, *delete*, *edit*, glob, *list*, *client-ssl*, *server-ssl*, *modify*, regex, *tmsh*

96

sys fpga

- Introducing the sys fpga module
- Alphabetical list of components

Introducing the sys fpga module

You can use the tmsh components that reside within the sys fpga module to manage FPGA objects on the system. For more information about the tmsh hierarchical structure, see Chapter 2, *Understanding and Using the Traffic Management Shell*.

Alphabetical list of components

The remainder of this chapter lists the tmsh components that are available in the sys fpga module.

firmware-config

Configures the FPGA firmware to be used by the system.

Syntax

Configure the **firmware-config component** within the **sys fpga** module using the syntax shown in the following sections.

Modify

```
modify firmware-config
   type  [ l4-performance-fpga | l7-intelligent-fpga | standard-balanced-fpga ]
```

Display

```
list firmware-config
    all-properties
    non-default-properties
    one-line
```

Description

You can use the **firmware-config** component to configure the PFGA firmware type to use.

Examples

list firmware-config

Displays properties of the current FPGA firmware configuration.

modify firmware-config type

Modify the type of the current FPGA firmware configuration. The default is standard-balanced-fpga.

Options

- **type**
  The type for FPGA firmware current used on the system.
  l4-performance-fpga: High throughput fpga firmware.
  l7-intelligent-fpga: eFAD and L7 intelligent fpga firmware.
  standard-balanced-fpga: The balanced standard fpga firmware.

See Also

list, *modify*, *tmsh*, fpga

info

Displays current FPGA (Field-Programmable Gate Array) firmware information on the system.

Syntax

Displays current **info** component within the **sys fpga** module using the syntax in the following section.

Display

```
show info
    all-properties
    field-fmt
```

Description

You can use the **info** component to display the current FPGA firmware information on the system.

Examples

show info

Displays current FPGA (Field-Programmable Gate Array) firmware information on the system

See Also

show, *tmsh*, fpga

97

sys icall

- Introducing the sys icall module
- Alphabetical list of components

Introducing the sys icall module

You can use the tmsh components that reside within the sys icall module to manage icall objects on the system. For more information about the tmsh hierarchical structure, see Chapter 2, *Understanding and Using the Traffic Management Shell*.

Alphabetical list of components

The remainder of this chapter lists the tmsh components that are available in the sys icall module.

event

Generate an Event on the BIG-IP® system.

Syntax

Generate the event component within the **sys icall** module using the syntax shown in the following sections.

Generate

```
generate event
  name [string]
  context {
   {
    name [string]
    value [string}
   }
  }
```

Description

You may use the generate event command to construct a free-form Event in the system which will be sent to interested Event Handlers.

Examples

generate event name EMPLOYEE context { { first_name Sam } { last_name Shepard } }

Construct an event named "EMPLOYEE" that contains two pieces of information as
name/value pairs. An Event Handler must be subscribed to the event by the name
"EMPLOYEE" or by both event name and all the contexts in a context group.

Options

- **context**
  Specifies a set of name/value pairs that convey the information of the Event.
- **name**
  The Events name; does not have to be unique, but may not be empty.

See Also

create, *delete*, *edit*, *list*, *modify*, *show*, sys icall event-handler, *script*, *tmsh*

istats-trigger

Configure an iStats trigger to generate a user defined event for the iCall feature on the BIG-IP® system.

Syntax

Modify the istats-trigger component within the **sys icall** module using the syntax shown in the following sections.

Create/Modify

```
create istats-trigger [name]
modify istats-trigger [name]
  description [string]
  duration [integer]
  event-name [string]
  istats-key [string]
  range-max [integer]
  range-min [integer]
  repeat [integer]
mv istats-trigger [ [ [source-name] [destination-name] ]    |
                    [ [name] to-folder [folder-name] ]      |
                    [ [name...name] to-folder [folder-name] ] ]
    to-folder
```

Display

```
list istats-trigger
list istats-trigger [ [ [name] | [glob] | [regex] ] ... ]
```

Delete

```
delete istats-trigger [name]
```

Description

You can create an istats-trigger to automatically generate a Control Plane iRules event under the conditions specified in the properties.

Examples

mv istats-trigger /Common/my_istats_trigger to-folder /Common/my_folder

Moves an istats-trigger named **my_istats_trigger** to a folder named **my_folder**, where **my_folder** has already been created and exists within **/Common**.

Options

- **description**
  A user defined description of the item.
- **duration**
  Duration in seconds. The value "0" means trigger instantly when in range.
- **event-name**
  The name of the event that will be generated.
- **istats-key**
  Specify the items and thresholds to define when this istats-trigger will generate an event.
- **range-max**
  Trigger event only if value is less-than-or-equal to range-max.
- **range-min**
  Trigger event only if value is greater-than-or-equal to range-min. Note that if 0 is included in the specified range, then the iStats key must be explicitly initialized with istats set [key] 0 in order for the trigger to fire.
- **repeat**
  Repeat interval in seconds. The value "none" means do not resend the event unless the value falls outside the range and then re-enters it.
- **to-folder**
  An **istats-trigger** can be moved to any folder under **/Common**, but configuration dependencies may restrict it from moving out of **/Common**.

See Also

create, *delete*, *edit*, *list*, *modify*, *mv*, *show*, *event*, sys icall event-handler, *script*, *tmsh*

publisher

show the services publishing events on a BIG-IP® system

Syntax

Show the available publishers within the **sys icall** module using the syntax shown in the following sections.

Display

```
show publisher [ field-fmt ]
show publisher [ [ [name] | [glob] | [regex] ] ... ] [ field-fmt ]
```

Description

This command lets you display the publishers on the system, as well as the events that they publish and the contexts that those events are guaranteed to contain.

By default these are shown in a tabular form; use the **field-fmt** option to show them in a format similar to listing other objects in tmsh.

If a published event includes no contexts, then a single line will be shown with a **-** in the context column. If a publisher publishes no events, then a single line will be shown with a **-** in the event column.

Options

- **field-fmt**
  By default, the events will be shown in a tabular format. This overrides the command to print the publishers in object format like the **list** command does for other objects.

See Also

show, *tmsh*, *event*, *periodic*, *perpetual*, *triggered*, *istats-trigger*, *script*

script

Manage a Tcl script used by handlers during execution on the BIG-IP® system.

Syntax

Manage the script component within the **sys icall** module using the syntax shown in the following sections.

Create/Modify/Edit

```
create script [name]
modify script [name]
edit script [name]
  definition
  description [string]
  events [add | delete | modify | replace-all-with] {
   [event name] {
   contexts [add | delete | modify | replace-all-with] {
    [context name]
    }
   }
  }
mv script [ [ [source-name] [destination-name] ]    |
            [ [name] to-folder [folder-name] ]      |
            [ [name...name] to-folder [folder-name] ] ]
    to-folder
```

Display

```
list script
list script [name]
```

Delete

```
delete script [name]
```

◆ Note

You must remove all references to the icall script before deletion.

Description

You can use this **script** component to manage Tcl scripts which are used by event handlers upon execution.

Caution: if you add a handler to a shared configuration on a set of BIG-IP appliances, then care must be used in making changes to configuration items. A handler's script which makes config changes on more than one device may cause inconsistencies that must be manually resolved.

Examples

create script my_script1

Create a new icall script item called "my_script1". Upon pressing enter, the user
will enter the text editor in order to edit the Tcl script. Note that this configuration item may only be modified while in the edit view.

mv script /Common/my_script to-folder /Common/my_folder

Moves an icall script named **my_script** to a folder named **my_folder**, where **my_folder** has already been created and exists within **/Common**.

Options

- **definition**
  Holds the Tcl code.
- **description**
  User defined description.
- **events**
  Register events with the system that this script creates.
- **to-folder**
  An icall **script** can be moved to any folder under **/Common**, but configuration dependencies may restrict it from moving out of **/Common**.

Event Accessors

In addition to all the **tmsh::** commands provided by the system to use in the Tcl scripts (please see help cli script), the commands below are provided to access event specific information.

Hint: When you use a **tmsh::** command, call it inside of Tcl **catch** to receive any error messages returned, and to allow the script to exit gracefully if needed. Without Tcl catch, the script may crash and end the process.

The following Tcl variables may be used in triggered handlers. (The **$** is not part of the variable name but is the lookup operator for the Tcl variable.):

$EVENT::context([name])

An array variable containing the value of each context, keyed by the context name.

$EVENT::creation_time

The date and time the event was generated.

$EVENT::event_name

The name of the event that was generated.

$EVENT::handler_name

The name of the event handler that matched the event being handled.

$EVENT::script_name

The name of the currently running script.

For use in perpetual handlers:

EVENT::get_next [-timeout [milliseconds]]

The timeout parameter is optional. If the timeout is set, then **EVENT::get_next** will return 0 if no event matches before the timeout hits. Otherwise, the **EVENT::get_next** will return 1, and the above variables in the **EVENT::** namespace will be replaced with the data from the new event.

Script Examples

The following script will print out all the information of an event.

```
puts "*** start of event ***"

foreach var [info vars EVENT::*] { set varname [namespace tail $var] if { [array exists $var] } { puts "$varname: " foreach { k v } [array get $var] { ;#k = key v = value puts "$k:$v" } } else { puts "$varname: [set $var]" } }
```

The next script will allow events to hold bash commands and have the script execute them. The script would be required to run inside an event handler that subscribed to the appropriate event and filtered on the words "utility" and "arguments".

```
set bash_cmd $EVENT::context(utility) append bash_cmd " " $EVENT::context(arguments)

if { [catch { exec /bin/bash -c $bash_cmd } result] } { puts "error executing bash command: $bash_cmd" } else { puts $result }
```

See Also

script, *create*, *delete*, *edit*, *list*, *modify*, *show*, *event*, sys icall event-handler, *tmsh*

98

sys icall handler

- Introducing the sys icall handler module
- Alphabetical list of components

Introducing the sys icall handler module

You can use the tmsh components that reside within the sys icall handler module to manage icall-handler objects on the system. For more information about the tmsh hierarchical structure, see Chapter 2, *Understanding and Using the Traffic Management Shell*.

Alphabetical list of components

The remainder of this chapter lists the tmsh components that are available in the sys icall handler module.

periodic

make or configure a periodic handler for the BIG-IP® system.

Syntax

Modify the periodic component within the **sys icall handler** module using the syntax shown in the following sections.

Create/Modify

```
create periodic [name]
modify periodic [name]
  arguments {
   {
     name [string]
     value [string]
   }
   ...
  }
  description [string]
  first-occurrence [date/time]
  interval [integer]
  last-occurrence [date/time]
  script [script name]
  status [active | inactive]
mv periodic [ [ [source-name] [destination-name] ]    |
              [ [name] to-folder [folder-name] ]      |
              [ [name...name] to-folder [folder-name] ] ]
    to-folder
```

Display

```
list periodic
list periodic [ [ [name] | [glob] | [regex] ] ... ]
show periodic
show periodic [ [ [name] | [glob] | [regex] ] ... ]
```

Delete

```
delete periodic [name]
```

Description

You can create a periodic handler to run scripts automatically based on clock time.

Examples

create periodic my_handler1 script script1 first-occurrence now+1h interval 45 arguments { { name user value j.han } { name role value manager } }

Create a new periodic handler that will execute script1 every 45 seconds. The
handler will wait one hour before beginning, but continue to execute indefinitely. Each 45 seconds, when the script executes, the provided arguments
will be passed into the script as EVENT::context(<name>) data.

mv periodic /Common/my_periodic to-folder /Common/my_folder

Moves a periodic icall handler named **my_periodic** to a folder named **my_folder**, where **my_folder** has already been created and exists within **/Common**.

Options

- **arguments**
  Specifies a set of name/value pairs that will be passed to the script at the start of each execution on each interval.
  The use of arguments is optional and may be changed at any time.
- **description**
  A user defined description of the item.
- **first-occurrence**
  A specific date and time for this handler to begin executing. If not specified, the current date and time of creation will be used.
- **interval**
  The number of seconds between each time this handler should execute.
- **last-occurrence**
  A specific date and time for this handler to stop executing. If not specified, the script will run indefinitely.
- **script**
  The iCall Tcl script the handler when execute at each time interval. Note that this script must be an object in **sys icall script**; a **cli script** will not work.
- **status**
  Specify either active or inactive. Active is the default value.
  When the handler status is active, the handler accepts events and executes the script as expected. However, when the status is inactive, the handler will no longer accept incoming events and the script will not execute. Use the inactive status when you wish to keep the handler as a configuration item and do not wish to delete it, but also do not wish the handler to run.

- **to-folder**
  A **periodic** icall handler can be moved to any folder under **/Common**, but configuration dependencies may restrict it from moving out of **/Common**.

See Also

create, *delete*, *edit*, *list*, *modify*, *mv*, *show*, *event*, *script*, *tmsh*

perpetual

make or configure a perpetual handler for the BIG-IP® system.

Syntax

Modify the perpetual component within the **sys icall handler** module using the syntax shown in the following sections.

Create/Modify

```
create perpetual [name]
modify perpetual [name]
  description [string]
  script [script name]
  status [active | inactive | suspend ]
  subscriptions [add | delete | modify | replace-all-with] {
   [subscription name] {
     event-name [event name]
     filters [add | delete | modify | replace-all-with] {
      [filter name] {
        value [string]
        match-algorithm [accept-all | exact | glob | regex | subnet]
      }
     }
   }
  }
restart perpetual [name]
start perpetual [name]
stop perpetual [name]
mv perpetual [ [ [source-name] [destination-name] ]    |
               [ [name] to-folder [folder-name] ]      |
               [ [name...name] to-folder [folder-name] ] ]
    to-folder
```

Display

```
list perpetual
list perpetual [ [ [name] | [glob] | [regex] ] ... ]
show perpetual
show perpetual [ [ [name] | [glob] | [regex] ] ... ]
```

Delete

```
delete perpetual [name]
```

Description

You can create a perpetual handler to run continuously executing code and to receive events by specifying subscriptions.

Examples

create perpetual my_handler1 script script1 subscriptions add { sub1 { event-name LTM_POOL_UP } }

Creates a new perpetual handler run the program defined in "script1". Anytime
an event called "LTM_POOL_UP" is generated in the system, a copy will be sent
to my_handler1.

mv perpetual /Common/my_perpetual to-folder /Common/my_folder

Moves a perpetual icall handler named **my_perpetual** to a folder named **my_folder**, where **my_folder** has already been created and exists within **/Common**.

Options

- **description**
  A user defined description of the item.
- **script**
  The iCall Tcl script the handler will execute upon creation. The user is responsible for creating a script with perpetual execution. If the script is changed, the handler will not change its executing code until the handler is restarted or put into inactive and then active status.
  Note that this script must be an object in **sys icall script**; a **cli script** will not work.
- **status**
  Specify active, inactive, or suspend. Active is the default value.
  Inactive status indicated that the handler is to no longer execute and to no longer receive events. The handler's state is lost and all pending events are deleted. Use this status to eliminate a handler in the system but to keep its information stored.
  The handler may also be set to suspend which will keep the handler script executing, but the system will send no new events to the handler. Events waiting to be processed remain in queue.
- **subscriptions**
  Create one or more subscription items to specify the conditions of this handler's execution. The handler subscribes generally to events by the event name, and specifically to data by using filters. The use of filters is optional.
  The handler will be sent events by the system as defined by the subscription property, but the code inside the handler must use EVENT::get_next function in order to receive the data into the handler. See sys icall script for more information.
- **to-folder**
  A **perpetual** icall handler can be moved to any folder under **/Common**, but configuration dependencies may restrict it from moving out of **/Common**.

See Also

create, *delete*, *edit*, *list*, *modify*, *mv*, *show*, *event*, *script*, *tmsh*

triggered

make or configure an event-triggered handler for the BIG-IP® system.

Syntax

Modify the triggered component within the **sys icall handler** module using the syntax shown in the following sections.

Create/Modify

```
create triggered [name]
modify triggered [name]
  description [string]
  script [script name]
  status [active | inactive]
  subscriptions [add | delete | modify | replace-all-with] {
   [subscription name] {
     event-name [event name]
     filters [add | delete | modify | replace-all-with] {
      [filter name] {
        value [string]
        match-algorithm [accept-all | exact | glob | regex | subnet]
      }
     }
   }
  }
mv triggered [ [ [source-name] [destination-name] ]    |
               [ [name] to-folder [folder-name] ]      |
               [ [name...name] to-folder [folder-name] ] ]
    to-folder
```

Display

```
list triggered
list triggered [ [ [name] | [glob] | [regex] ] ... ]
show triggered
show triggered [ [ [name] | [glob] | [regex] ] ... ]
```

Delete

```
delete triggered [name]
```

Description

You can create a triggered handler to automatically run a script when a specified event occurs.

Examples

create triggered my_handler1 script script1 subscriptions add { pools { event-name LTM_POOL_UP filters add { pool_name { value pool1 } node_name { value node1 } } } }

Creates a new triggered handler that will execute the script called "script1" when an event called "LTM_POOL_UP" is generated in the system and
contains the contexts { pool_name, pool1 } and { node_name, node1 }.

mv triggered /Common/my_triggered to-folder /Common/my_folder

Moves a triggered icall handler named **my_triggered** to a folder named **my_folder**, where **my_folder** has already been created and exists within **/Common**.

Options

- **description**
  A user defined description of the item.
- **script**
  The iCall Tcl script the handler will execute when invoked by an appropriate event. Note that this script must be an object in **sys icall script**; a **cli script** will not work.
- **status**
  Specify either active or inactive. Active is the default value.
  When the handler status is active, the handler accepts events and executes the script as expected. However, when the status is inactive, the handler will no longer accept incoming events and the script will not execute. Use the inactive status when you wish to keep the handler as a configuration item and do not wish to delete it, but also do not wish the handler to run.
- **subscriptions**
  Specify one or more subscriptions to define the conditions of this handler's execution. The handler subscribes generally to events by the event name, and specifically to data by using filters. The use of filters is optional.
  A handler that specifies more than one subscription will execute when any one subscription is matched to an event.
- **to-folder**
  A **triggered** icall handler can be moved to any folder under **/Common**, but configuration dependencies may restrict it from moving out of **/Common**.

See Also

create, *delete*, *edit*, *list*, *modify*, *mv*, *show*, *event*, *script*, *tmsh*

99

sys ipfix

- Introducing the sys ipfix module
- Alphabetical list of components

Introducing the sys ipfix module

You can use the tmsh components that reside within the sys ipfix module to manage IPFIX objects on the system. For more information about the tmsh hierarchical structure, see Chapter 2, *Understanding and Using the Traffic Management Shell*.

Alphabetical list of components

The remainder of this chapter lists the tmsh components that are available in the sys ipfix module.

destination

Displays or resets statistics for IPFIX log destinations.

Syntax

Specify the **destination** within the **sys ipfix** module using the syntax in the following section.

Modify

```
reset-stats destination [name]
```

Display

```
show destination [name]
```

Description

You can use the **destination** component to display IPFIX destination statistics, like Templates and Data Record counts. You can also reset the IPFIX destination statistics to zero at any time.

Options

For information about the options that you can use with the command **show**, see **help show**.

For information about the options that you can use with the command **reset-stats**, see **help reset-stats**.

See Also

reset-stats, *show*, *ipfix*, *irules*, *element*, *tmsh*

element

Configures element for IPFIX logging.

Syntax

Configure the IPFIX component within the **sys ipfix** module using the syntax shown in the following sections.

Create/Modify

```
create element [name]
modify element [name]
  all
  app-service [[string] | none]
  data-type
     [ boolean | datetime-microseconds |
       datetime-milliseconds | datetime-nanoseconds |
       datetime-seconds | float32 | float64 |
       ipv4-address | ipv6-address | macaddress |
       octetarray | signed16 | signed32 | signed64 |
       signed8 | string |
       unsigned16 | unsigned32 |
       unsigned64 | unsigned8 ]
  description [string]
  enterprise-id [integer]
  id [integer]
  size [integer]
```

Display

```
list element
list element [ [ [name] | [glob] | [regex] ] ... ]
    all-properties
    non-default-properties
    one-line
```

Delete

```
delete element [name]
```

Note

Default elements loaded at boot time may not be deleted.

Description

You can use the **element** component to configure elements for the IPFIX logging interface.

Examples

create element myelement id 345 enterprise-id 543 data-type string size 128

Creates a element named **myelement** with element id **345**, enterprise-id **543**,
data-type **string** and data size of **128**.

delete element myelement

Deletes the element named **myelement**.

list element myelement

Displays properties of the element named **myelement**.

Options

- **all**
  Specifies that you want to modify all of the existing components of the specified type.
- **app-service**
  Specifies the name of the application service to which the element belongs. The default value is **none**. **Note:** If the **strict-updates** option is **enabled** on the application service that owns the object, you cannot modify or delete the element. Only the application service can modify or delete the element.
- **data-type**
  Specifies the data type of the element.
- **description**
  User defined description.
- **enterprise-id**
  Specifies the enterprise-id for the IPFIX element being configured between 0 and 4294967295. An enterprise id value of 0 is used to define standardized IANA Information Elements.
- **id**
  Specifies the element id for the IPFIX element being configured between 1 and 65535. Values greater than 32767 will be considered NETFLOW-only Information Elements; since the high bit of the 16-bit value is set for those values.
- **size**
  Specifies the IPFIX element data size between 1 and 1900 for data-types octetarray and string. The default is 0; and means variable for these two data-types.
- **glob**
  Displays the items that match the **glob** expression. See **help glob** for a description of **glob** expression syntax.

- **name**
  Specifies a unique alphanumeric name for the component. Preferably camel casing. This option is required for the commands **create**, **delete**, and **modify**.
- **regex**
  Displays the items that match the regular expression. The regular expression must be preceded by an at sign (@[regular expression]) to indicate that the identifier is a regular expression. See **help regex** for a description of regular expression syntax.

See Also

create, *delete*, glob, *list*, *modify*, regex, *tmsh*

irules

Displays or resets statistics for irules that use IPFIX logging destinations.

Syntax

Specify the **irules** component within the **sys ipfix** module using the syntax in the following section.

Modify

```
reset-stats irules
```

Display

```
show irules
```

Description

You can use the **irules** component to display a global set of statistics for the iRules that use IPFIX destinations, like memory allocation and outstanding counts for templates, messages and destinations. You can also reset the IPFIX iRules statistics to zero at any time.

Options

For information about the options that you can use with the command **show**, see **help show**.

For information about the options that you can use with the command **reset-stats**, see **help reset-stats**.

See Also

reset-stats, *show*, *ipfix*, *destination*, *element*, *tmsh*

100

sys log-config

- Introducing the sys log-config module
- Alphabetical list of components

Introducing the sys log-config module

You can use the tmsh components that reside within the sys log-config module to manage log configuration on the system. For more information about the tmsh hierarchical structure, see Chapter 2, *Understanding and Using the Traffic Management Shell*.

Alphabetical list of components

The remainder of this chapter lists the tmsh components that are available in the sys log-config module.

filter

Configures the filter component which filters out log messages for distribution by the publisher component.

Syntax

Configure the filter component within the **sys log-config** module using the syntax shown in the following sections.

Create/Modify

```
create filter [name]
modify filter [name]
  all
  app-service [[string] | none]
  description [string]
  level       [ alert | crit | debug | emerg | err | info | notice | warn ]
  message-id  [ 8 digit hex number | none ]
  publisher   [[string] | none]
  source      [ accesscontrol | adapt | alertd | all | apmacl | arp | avr |
                based | bcm56xxd | big3d | big3dshim | bigd | bigdb |
                bigdbd | bigpipe | bigstart | bp | checkcert |
                chmand | cifs | clusterd | coapi | common |
                common-f5logging | common-fpdd | config-db | connapi | cs |
                cssd | csyncd | daemon | deflate | devmgmtd | diameter |
                 dmon | dosprotect | dummy | eca | em-admin | em-alert |
                em-clientlib | em-common | em-device | em-discovery |
                em-file | em-lib | em-report | em-stats | em-swim | eventd |
                evrouted | fflag | get-dossier | gtmd | ha | ha-table |
                halmsg | http | hwctl | ip | iprepd | isession | istatsd |
                lacpd | layer4 | libhal | lind | lldp | mapi | mcp | mcpd |
                mgmt-acld | mysqlhad | net | network | no-source | packet-filter |
                pccd | pfmand | pktclass | plugin | portal-access | probe-plusplus |
                promptstatusd | pva | pvad | radius | ramcache | rba | rtsp |
                rules | saspd | scriptd | shell | snmp | sod | ssl | sso |
                statsd | stpd | subagents | syscall | system-check | tamd |
                tcl-checker | tcpdump | tmm | tmsh | ts | vcmpd | websso |
                woc-plugin | xconfig | xdb | zfd | zxfrd ]
```

Display

```
list filter
list filter [ [ [name] | [glob] | [regex] ] ... ]
    all-properties
    non-default-properties
    one-line
```

Delete

```
delete filter [name]
```

Description

You can use the **filter** component to configure the filters for the common logging interface.

Examples

create filter my_filt publisher my_pub

Creates a filter named **my_filt** with the publisher my_pub.

delete filter my_filt

Deletes the filter named **my_filt**.

list filter my_filt

Displays properties of the filter named **my_filt**.

Options

- **all**
  Specifies that you want to modify all of the existing components of the specified type.
- **app-service**
  Specifies the name of the application service to which the filter belongs. The default value is **none**. **Note:** If the **strict-updates** option is **enabled** on the application service that owns the object, you cannot modify or delete the filter. Only the application service can modify or delete the filter.
- **description**
  User defined description.
- **glob**
  Displays the items that match the **glob** expression. See **help glob** for a description of **glob** expression syntax.
- **level**
  The minimum severity level of logs to be filtered. The severity levels in increasing order are debug, info, notice, warn, err, crit, alert, and emerg. The default value is **debug**.
- **message-id**
  A refinement for filtering out specific logs. The default value is **none**. This is an eight digit hex number. The proper hex value can be obtained from an existing log message by extracting the eight digit value.
  For example, the message-id for the example log message below is highlighted.
  Oct 9 15:38:20 bigip1 notice mcpd[21498]: **01070410**:5: Removed subscription with subscriber id logstatd
- **name**
  Specifies a unique name for the component. This option is required for the commands **create**, **delete**, and **modify**.

- **publisher**
  A publisher to send filtered log messages. The default value is **none**.
- **regex**
  Displays the items that match the regular expression. The regular expression must be preceded by an at sign (@[regular expression]) to indicate that the identifier is a regular expression. See **help regex** for a description of regular expression syntax.
- **source**
  The stream of log messages that will be filtered by the created/modified filter. The default value is **all**.

See Also

create, *delete*, glob, *list*, *modify*, regex, *tmsh*

publisher

Configures lists of destinations for the common logging interface.

Syntax

Configure the publisher component within the **sys log-config** module using the syntax shown in the following sections.

Create/Modify

```
create publisher [name]
modify publisher [name]
  all
  app-service [[string] | none]
  description [string]
  destinations [add | delete | none | replace-all-with] {
     [ [destinations] ]
  }
```

Display

```
list publisher
list publisher [ [ [name] | [glob] | [regex] ] ... ]
    all-properties
    non-default-properties
    one-line
```

Delete

```
delete publisher [name]
```

Note

You must remove all references to a publisher before you can delete the publisher. Default publishers may not be deleted.

Description

You can use the **publisher** component to configure publishers for the common logging interface.

Examples

create publisher my_pub destinations add {
destination_1
destination_2
}

Creates a publisher named **my_pub** with two destinations, **destination_1**

delete publisher my_pub

Deletes the publisher named **my_pub**.

list publisher my_pub

Displays properties of the publisher named **my_pub**.

Options

- **all**
  Specifies that you want to modify all of the existing components of the specified type.
- **app-service**
  Specifies the name of the application service to which the publisher belongs. The default value is **none**. **Note:** If the **strict-updates** option is **enabled** on the application service that owns the object, you cannot modify or delete the publisher. Only the application service can modify or delete the publisher.
- **description**
  User defined description.
- **destinations**
  Adds, deletes, or replaces a set of destinations.
- **glob**
  Displays the items that match the **glob** expression. See **help glob** for a description of **glob** expression syntax.
- **name**
  Specifies a unique name for the component. This option is required for the commands **create**, **delete**, and **modify**.
- **regex**
  Displays the items that match the regular expression. The regular expression must be preceded by an at sign (@[regular expression]) to indicate that the identifier is a regular expression. See **help regex** for a description of regular expression syntax.

See Also

create, *delete*, glob, *list*, *modify*, regex, *tmsh*

101

sys log-config destination

- Introducing the sys log-config destination module
- Alphabetical list of components

Introducing the sys log-config destination module

You can use the tmsh components that reside within the sys log-config destination module to manage remote-log configuration. For more information about the tmsh hierarchical structure, see Chapter 2, *Understanding and Using the Traffic Management Shell*.

Alphabetical list of components

The remainder of this chapter lists the tmsh components that are available in the sys log-config destination module.

alertd

Modify the AlertD destination.

Syntax

Modify the AlertD component within the **sys log-config destination** module using the syntax shown in the following sections.

Modify

```
modify alertd [name]
options:
 all
 description [string]
```

Display

```
list alertd
list alertd [ [ [name] | [glob] | [regex] ] ... ]
    all-properties
    non-default-properties
    one-line
```

◆ Note

There is only one AlertD destination, alertd; this destination cannot be created or deleted.

Description

You can use this **destination** component to modify the AlertD destination for the common logging interface. There is only one AlertD destination; it cannot be deleted. You can use this destination to send logs directly to the AlertD daemon, bypassing syslog-ng.

Examples

list alertd alertd

Displays properties of the AlertD destination.

Options

- **all**
  Specifies that you want to modify all of the existing components of the specified type.

- **description**
  User defined description.
- **glob**
  Displays the items that match the **glob** expression. See **help glob** for a description of **glob** expression syntax.
- **name**
  Specifies a unique name for the component. This option is required for the **modify** command.
- **regex**
  Displays the items that match the regular expression. The regular expression must be preceded by an at sign (@[regular expression]) to indicate that the identifier is a regular expression. See **help regex** for a description of regular expression syntax.

See Also

glob, *list*, *modify*, regex, *tmsh*

arcsight

Formats incoming logs into the ArcSight format for delivery by a forwarding destination.

Syntax

Configure the ArcSight component within the **sys log-config destination** module using the syntax shown in the following sections.

Create/Modify

```
create arcsight [name]
modify arcsight [name]
  all
  app-service [[string] | none]
  description [string]
  forward-to [string]
```

Display

```
list arcsight
list arcsight [ [ [name] | [glob] | [regex] ] ... ]
    all-properties
    non-default-properties
    one-line
```

Delete

```
delete arcsight [name]
```

◆ Note

You must remove all references to a destination before you can delete the destination. Default destinations may not be deleted.

Description

You can use this **destination** component to create ArcSight formatting destinations for the common logging interface. ArcSight log destinations currently only deliver log messages from the Network Firewall Module or the Application Security Module.

Examples

create arcsight my_dest forward-to another_dest

Creates an ArcSight destination named **my_dest** which forwards to another destination another_dest. another_dest must be a Local Syslog, Local Database,
Remote Syslog, or Remote High Speed Log destination.

delete arcsight my_dest

Deletes the destination named **my_dest**. Destinations cannot be deleted when
in use by a publisher.

list arcsight my_dest

Displays properties of the destination named **my_dest**.

Options

- **all**
  Specifies that you want to modify all of the existing components of the specified type.
- **app-service**
  Specifies the name of the application service to which the destination belongs. The default value is **none**. **Note:** If the **strict-updates** option is **enabled** on the application service that owns the object, you cannot modify or delete the destination. Only the application service can modify or delete the destination.
- **description**
  User defined description.
- **forward-to**
  Specifies a Local Syslog, Local Database, Remote Syslog, or Remote High Speed Log destination. This is required for the **create** and **modify** commands.
- **glob**
  Displays the items that match the **glob** expression. See **help glob** for a description of **glob** expression syntax.
- **name**
  Specifies a unique name for the component. This option is required for the commands **create**, **delete**, and **modify**.
- **regex**
  Displays the items that match the regular expression. The regular expression must be preceded by an at sign (@[regular expression]) to indicate that the identifier is a regular expression. See **help regex** for a description of regular expression syntax.

See Also

create, *delete*, glob, *list*, *modify*, regex, *tmsh*

ipfix

Formats log messages into IPFIX messages and sends them to a specified pool of IPFIX Collectors

Syntax

Create/Modify

```
create ipfix [name]
modify ipfix [name]
  all
  app-service                    [[string] | none]
  description                    [string]
  pool-name                      [string]
  protocol-version               [ipfix | netflow-9]
  template-delete-delay          [integer]
  template-retransmit-interval   [integer]
  transport-profile              [profile name]
  serverssl-profile              [profile name]
```

Display

```
list ipfix
list ipfix [ [ [name] | [glob] | [regex] ] ... ]
    all-properties
    non-default-properties
    one-line
```

Delete

```
delete ipfix [name]
```

◆ Note

You must remove all references to a destination before you can delete the destination. Default destinations may not be deleted.

Description

You can use this **destination** component to create IPFIX forwarding destinations for the common logging interface.

The IPFIX protocol is designed for logging IP-transmission events. RFC 5101 (http://tools.ietf.org/html/rfc5101) specifies the protocol, and RFC 5102 (http://tools.ietf.org/html/rfc5102) describes the information model for IPFIX logs. IPFIX logs are raw, binary-encoded strings with their fields and field lengths defined by *IPFIX templates*. *IPFIX collectors* are external devices that can receive IPFIX templates and use them to interpret IPFIX logs.

Examples

create ipfix my_dest pool-name my_pool

Creates a destination named **my_dest** which sends IPFIX messages to the pool named **my_pool**.

delete ipfix my_dest

Deletes the destination named **my_dest**. Destinations cannot be deleted when in use by a publisher or another destination.

list ipfix my_dest

Displays properties of the destination named **my_dest**.

Options

- **all**
  Specifies that you want to modify all of the existing components of the specified type.
- **app-service**
  Specifies the name of the application service to which the destination belongs. The default value is **none**.
  Note: If the **strict-updates** option is **enabled** on the application service that owns the object, you cannot modify or delete the destination. Only the application service can modify or delete the destination.
- **description**
  A user defined description for this logging destination.
- **glob**
  Displays the items that match the **glob** expression. See **help glob** for a description of **glob** expression syntax.
- **name**
  Specifies a unique name for the component. This option is required for the commands **create**, **delete**, and **modify**.
- **pool-name**
  Specifies the LTM pool that receives messages from the IPFIX destination. This option is required for the **create** command. The pool should contain one or more IPFIX collectors; use the *pool* component to set up an LTM pool.
- **protocol-version**
  Specifies the protocol version used to encode IPFIX messages sent by this logging destination. The possible values are ipfix and netflow-9. The default is **ipfix**.
- **template-delete-delay**
  This feature is not implemented.
- **template-retransmit-interval**
  Specifies the time interval, in seconds, after which this IPFIX logging destination must resend all active IPFIX Templates to the pool of IPFIX collectors.
  The logging destination periodically retransmits all of its IPFIX

templates at the interval you set in this property. These retransmissions can be helpful if the **transport-profile** is UDP, a lossy transport mechanism. They can also be useful for debugging a network session with a network analyzer, such as Wireshark.
The default value is 30 seconds.

- **transport-profile**
  Specifies the name of a profile for the transport protocol to be used by this IPFIX logging destination. You can use any existing TCP-based or UDP-based profile. The default value is the default udp profile.
  You can use the **ltm profile tcp** command (see *tcp*) to create a TCP profile, or **ltm profile udp** (see *udp*) to create a UDP profile.
- **serverssl-profile**
  Specifies the name of a server-side SSL profile to be used by this IPFIX Log Destination. The default is not to use a server-side SSL profile. If one is specified, the IPFIX Log Destination must be configured to use TCP as the transport protocol, and will use SSL over TCP to communicate with the configured IPFIX collectors.
  You can use the **ltm profile server-ssl** command (see *server-ssl*) to create a server-side SSL profile.
- **regex**
  Displays the items that match the regular expression. The regular expression must be preceded by an at sign (@[regular expression]) to indicate that the identifier is a regular expression. See **help regex** for a description of regular expression syntax.

See Also

pool, *tcp*, *udp*, *create*, *delete*, glob, *list*, *modify*, regex, *tmsh*

local-database

Modify the Local Database destination.

Syntax

Modify the Local Database component within the **sys log-config destination** module using the syntax shown in the following sections.

Modify

```
modify local-database [name]
options:
 all
 description [string]
```

Display

```
list local-database
list local-database [ [ [name] | [glob] | [regex] ] ... ]
    all-properties
    non-default-properties
    one-line
```

◆ Note

There is only one Local Database destination, local-db. This destination cannot be created or deleted.

Description

You can use this **destination** component to modify the Local Database destination for the common logging interface. There is only one Local Database destination that cannot be deleted.

Examples

list local-database local-db

Displays properties of the Local Database destination.

Options

- **all**
  Specifies that you want to modify all of the existing components of the specified type.
- **description**
  User defined description.

- **glob**
  Displays the items that match the **glob** expression. See **help glob** for a description of **glob** expression syntax.
- **name**
  Specifies a unique name for the component. This option is required for the **modify** command.
- **regex**
  Displays the items that match the regular expression. The regular expression must be preceded by an at sign (@[regular expression]) to indicate that the identifier is a regular expression. See **help regex** for a description of regular expression syntax.

See Also

glob, *list*, *modify*, regex, *tmsh*

local-syslog

Configures the Local Syslog destination.

Syntax

Modify the Local Syslog component within the **sys log-config destination** module using the syntax shown in the following sections.

Modify

```
modify local-syslog [name]
options:
 all
 default-facility [ local0 | local1 | local2 | local3 | local4 | local5 | local6 |
local7 ]
 default-severity [ alert | crit | debug | emerg | err | info | notice | warn ]
 description [string]
```

Display

```
list local-syslog
list local-syslog [ [ [name] | [glob] | [regex] ] ... ]
    all-properties
    non-default-properties
    one-line
```

◆ Note

There is only one Local Syslog destination, local-syslog. This destination cannot be created or deleted.

Description

You can use this **destination** component to modify the Local Syslog destination for the common logging interface.There is only one Local Syslog destination which cannot deleted.

Examples

list local-syslog local-syslog

Displays properties of the Local Syslog destination.

Options

- **all**
  Specifies that you want to modify all of the existing components of the specified type.

- **default-facility**
  Specifies the facility given to log messages received that do not already have one. The default value is **local0**. The options are local0, local1, local2, local3, local4, local5, local6, and local7.
- **default-severity**
  Specifies the severity given to log messages received that do not already have one. The default value is **info**. The options are debug, info, notice, warn, err, crit, alert, and emerg.
- **description**
  User defined description.
- **glob**
  Displays the items that match the **glob** expression. See **help glob** for a description of **glob** expression syntax.
- **name**
  Specifies a unique name for the component. This option is required for the **modify** command.
- **regex**
  Displays the items that match the regular expression. The regular expression must be preceded by an at sign (@[regular expression]) to indicate that the identifier is a regular expression. See **help regex** for a description of regular expression syntax.

See Also

glob, *list*, *modify*, regex, *tmsh*

remote-high-speed-log

Sends received messages to a specified pool.

Syntax

Configure the Remote High Speed Log component within the **sys log-config destination** module using the syntax shown in the following sections.

Create/Modify

```
create remote-high-speed-log [name]
modify remote-high-speed-log [name]
  all
  app-service [[string] | none]
  description [string]
  pool-name [ string ]
  protocol [ tcp | udp ]
```

Display

```
list remote-high-speed-log
list remote-high-speed-log [ [ [name] | [glob] | [regex] ] ... ]
    all-properties
    non-default-properties
    one-line
```

Delete

```
delete remote-high-speed-log [name]
```

◆ Note

You must remove all references to a destination before you can delete the destination. Default destinations may not be deleted.

Description

You can use this **destination** component to create Remote High Speed Log forwarding destinations for the common logging interface.

Examples

create remote-high-speed-log my_dest pool-name my_pool

Creates a destination named **my_dest** which forwards to the pool my_pool.

delete remote-high-speed-log my_dest

Deletes the destination named **my_dest**. Destinations cannot be deleted when
in use by a publisher or another destination.

list remote-high-speed-log my_dest

Displays properties of the destination named **my_dest**.

Options

- **all**
  Specifies that you want to modify all of the existing components of the specified type.
- **app-service**
  Specifies the name of the application service to which the destination belongs. The default value is **none**. **Note:** If the **strict-updates** option is **enabled** on the application service that owns the object, you cannot modify or delete the destination. Only the application service can modify or delete the destination.
- **description**
  User defined description.
- **glob**
  Displays the items that match the **glob** expression. See **help glob** for a description of **glob** expression syntax.
- **name**
  Specifies a unique name for the component. This option is required for the commands **create**, **delete**, and **modify**.
- **pool-name**
  Specifies the ltm pool that receives messages from the Remote High Speed Log destination. This option is required for the **create** command.
- **protocol**
  Specifies the protocol used to send messages to the specified pool. The default value is **tcp**. The options are tcp and udp.
- **regex**
  Displays the items that match the regular expression. The regular expression must be preceded by an at sign (@[regular expression]) to indicate that the identifier is a regular expression. See **help regex** for a description of regular expression syntax.

See Also

create, *delete*, glob, *list*, *modify*, regex, *tmsh*

remote-syslog

Configures Remote Syslog destinations to format log messages into Syslog format and forward them to a Remote High-Speed Log destination.

Syntax

Configure the Remote Syslog component within the **sys log-config destination** module using the syntax shown in the following sections.

Create/Modify

```
create remote-syslog [name]
modify remote-syslog [name]
  all
  app-service [[string] | none]
  default-facility [ local0 | local1 | local2 | local3 | local4 | local5 | local6 |
local7 ]
  default-severity [ alert | crit | debug | emerg | err | info | notice | warn ]
  description [string]
  format [ legacy-bigip | rfc3164 | rfc5424 ]
  remote-high-speed-log [string]
```

Display

```
list remote-syslog
list remote-syslog [ [ [name] | [glob] | [regex] ] ... ]
    all-properties
    non-default-properties
    one-line
```

Delete

```
delete remote-syslog [name]
```

◆ Note

You must remove all references to a destination before you can delete the destination. Default destinations may not be deleted.

Description

You can use this **destination** component to create Remote Syslog formatting destinations for the common logging interface.

Examples

create remote-syslog my_dest remote-high-speed-log another_dest

Creates a destination named **my_dest** which forwards to another destination another_dest. another_dest must be a Remote High Speed Log destination.

delete remote-syslog my_dest

Deletes the destination named **my_dest**. Destinations cannot be deleted when
in use by a publisher or another destination.

list remote-syslog my_dest

Displays properties of the destination named **my_dest**.

Options

- **all**
  Specifies that you want to modify all of the existing components of the specified type.
- **app-service**
  Specifies the name of the application service to which the destination belongs. The default value is **none**. **Note:** If the **strict-updates** option is **enabled** on the application service that owns the object, you cannot modify or delete the destination. Only the application service can modify or delete the destination.
- **default-facility**
  Specifies the facility given to log messages received that do not already have a facility listed. The default value is **local0**. The options are local0, local1, local2, local3, local4, local5, local6, and local7.
- **default-severity**
  Specifies the severity given to log messages received that do not already have a severity listed. The default value is **info**. The options are debug, info, notice, warn, err, crit, alert, and emerg.
- **description**
  User defined description.
- **format**
  Specifies the syslog format received messages are formatted into. The default value is **rfc3164**. The options are legacy-bigip, rfc3164, and rfc5424. For more information, see the respective RFCs.
- **glob**
  Displays the items that match the **glob** expression. See **help glob** for a description of **glob** expression syntax.
- **name**
  Specifies a unique name for the component. This option is required for the commands **create**, **delete**, and **modify**.
- **regex**
  Displays the items that match the regular expression. The regular expression must be preceded by an at sign (@[regular expression]) to indicate that the identifier is a regular expression. See **help regex** for a description of regular expression syntax.

- **remote-high-speed-log**
  Specifies the Remote High Speed Log destination. This option is required for the **create** command.

See Also

create, *delete*, glob, *list*, *modify*, regex, *tmsh*

splunk

Configures Splunk formatting destinations to format incoming log messages into the Splunk format.

Syntax

Configure the Splunk component within the **sys log-config destination** module using the syntax shown in the following sections.

Create/Modify

```
create splunk [name]
modify splunk [name]
  all
  app-service [[string] | none]
  description [string]
  forward-to [string]
```

Display

```
list splunk
list splunk [ [ [name] | [glob] | [regex] ] ... ]
    all-properties
    non-default-properties
    one-line
```

Delete

```
delete splunk [name]
```

◆ Note

You must remove all references to a destination before you can delete the destination. Default destinations may not be deleted.

Description

You can use this **destination** component to create Splunk formatting destinations for the common logging interface.

Examples

create splunk my_dest forward-to another_dest

Creates a destination named **my_dest** which forwards to another destination another_dest. another_dest must be a Local Syslog, Local Database, Remote Syslog, or Remote High Speed Log destination.

delete splunk my_dest

Deletes the destination named **my_dest**.

list splunk my_dest

Displays properties of the destination named **my_dest**. Destinations cannot be deleted when
in use by a publisher.

Options

- **all**
  Specifies that you want to modify all of the existing components of the specified type.
- **app-service**
  Specifies the name of the application service to which the destination belongs. The default value is **none**. **Note:** If the **strict-updates** option is **enabled** on the application service that owns the object, you cannot modify or delete the destination. Only the application service can modify or delete the destination.
- **description**
  User defined description.
- **forward-to**
  Specifies a Local Syslog, Local Database, Remote Syslog, or Remote High Speed Log destination to receive Splunk formatted log messages. This is required for the creation of a Splunk destination.
- **glob**
  Displays the items that match the **glob** expression. See **help glob** for a description of **glob** expression syntax.
- **name**
  Specifies a unique name for the component. This option is required for the commands **create**, **delete**, and **modify**.
- **regex**
  Displays the items that match the regular expression. The regular expression must be preceded by an at sign (@[regular expression]) to indicate that the identifier is a regular expression. See **help regex** for a description of regular expression syntax.

See Also

create, *delete*, glob, *list*, *modify*, regex, *tmsh*

102

sys performance

- Introducing the sys performance module
- Alphabetical list of components

Introducing the sys performance module

You can use the tmsh components that reside within the sys performance module to display statistics about the system. For more information about the tmsh hierarchical structure, see Chapter 2, *Understanding and Using the Traffic Management Shell*.

Alphabetical list of components

The remainder of this chapter lists the tmsh components that are available in the sys performance module.

all-stats

Resets or displays all performance statistics.

Syntax

Reset or display all performance statistics for the system within the **sys_performance** module using the syntax in the following sections. On VIPRION® systems, displaying performance statistics on a secondary blade is not supported.

Modify

```
reset-stats all-stats
```

Display

```
show all-stats
    (default | exa | gig | kil | meg | peta | raw | tera | yotta | zetta)
    (detail | historical)
```

Description

You can use the **all-stats** component to reset or display all system performance statistics.

Note that **tmsh** only displays performance statistics when you explicitly request them.

Examples

show all-stats detail

Displays detailed information about system performance in the system default units.

reset-stats all-stats

Resets all performance statistics for the system.

Options

For information about the options that you can use with the command **show**, see **help show**.

For information about the options that you can use with the command **reset-stats**, see **help reset-stats**.

See Also

reset-stats, *show*, *connections*, *gtm*, *ramcache*, *system*, *throughput*, *tmsh*

connections

Displays connection performance information.

Syntax

Display statistics for the **connections** component within the **sys performance** module using the syntax in the following section. On VIPRION® systems, displaying performance statistics on a secondary blade is not supported.

Display

```
show connections
    (default | exa | gig | kil | meg | peta | raw | tera | yotta | zetta)
    (detail | historical)
```

Description

You can use the **connections** component to display information about system performance, including details about new and active connections and HTTP requests.

You can reset the connection performance statistics using the **all-stats** component.

Examples

show connections gig detail

Displays detailed information about connection performance in gigabytes.

show connections historical

Displays historical performance information about connections.

Options

For information about the options that you can use with the command **show**, see **help show**.

See Also

show, *all-stats*, *gtm*, *ramcache*, *system*, *throughput*, *tmsh*

gtm

Displays performance information for the Global Traffic Manager.

Syntax

Display statistics for the **gtm** component within the **sys performance** module using the syntax in the following section. On VIPRION® systems, displaying performance statistics on a secondary blade is not supported.

Display

```
show gtm
    (default | exa | gig | kil | meg | peta | raw | tera | yotta | zetta)
    (detail | historical)
```

Description

You can use the **gtm** component to display information about system performance, including details about the Global Traffic Manager, including number of requests, resolutions, persisted connections, and those returned to DNS.

You can reset the Global Traffic Manager performance statistics using the **all-stats** component.

Examples

show gtm detail

Displays detailed performance information about the Global Traffic Manager in the system default units.

show gtm historical

Displays historical performance information about the Global Traffic Manager.

Options

For information about the options that you can use with the command **show**, see **help show**.

See Also

show, *all-stats*, *connections*, *ramcache*, *system*, *throughput*, *tmsh*

ramcache

Displays RAM cache performance information.

Syntax

Display statistics for the **ramcache** component within the **sys performance** module using the syntax in the following section. On VIPRION® systems, displaying performance statistics on a secondary blade is not supported.

Display

```
show ramcache
    (default | exa | gig | kil | meg | peta | raw | tera | yotta | zetta)
    historical
```

Description

You can use the **ramcache** component to display RAM cache utilization information.

You can reset the RAM cache performance statistics using the **all-stats** component.

Examples

show ramcache default

Displays ramcache performance information in the system default units.

show ramcache historical

Displays historical ramcache performance information.

Options

For information about the options that you can use with the command **show**, see **help show**.

See Also

show, *all-stats*, *connections*, *gtm*, *system*, *throughput*, *tmsh*

system

Displays system performance information.

Syntax

Display statistics for the **system** component within the **sys performance** module using the syntax in the following section. On VIPRION® systems, displaying performance statistics on a secondary blade is not supported.

Display

```
show system
    (default | exa | gig | kil | meg | peta | raw | tera | yotta | zetta)
    (detail | historical)
```

Description

You can use the **system** component to display CPU and memory usage information.

You can reset the system performance statistics using the **all-stats** component.

Examples

show system detail

Displays detailed system performance information in the system default units.

show system historical

Displays historical system performance information.

Options

For information about the options that you can use with the command **show**, see **help show**.

See Also

show, *all-stats*, *connections*, *gtm*, *ramcache*, *throughput*, *tmsh*

throughput

Displays performance information about traffic throughput.

Syntax

Display statistics for the **throughput** component within the **sys performance** module using the syntax in the following section. On VIPRION® systems, displaying performance statistics on a secondary blade is not supported.

Display

```
show throughput
    (default | exa | gig | kil | meg | peta | raw | tera | yotta | zetta)
    (detail | historical)
```

Description

You can use the **throughput** component to display information about traffic throughput, including client, server, compression, and SSL transactions.

You can reset the throughput performance statistics using the **all-stats** component.

Examples

show throughput gig detail

Displays detailed throughput performance information in gigabits per second.

show throughput historical

Displays historical throughput performance information.

Options

For information about the options that you can use with the command **show**, see **help show**.

See Also

show, *all-stats*, *connections*, *gtm*, *ramcache*, *system*, *tmsh*

103

sys raid

- Introducing the sys raid module
- Alphabetical list of components

Introducing the sys raid module

You can use the tmsh components that reside within the sys raid module to configure disk arrays and display information about the system arrays, bay, and disks. For more information about the tmsh hierarchical structure, see Chapter 2, *Understanding and Using the Traffic Management Shell*.

Alphabetical list of components

The remainder of this chapter lists the tmsh components that are available in the sys raid module.

array

Configures an array of hard disks on the BIG-IP® system.

Syntax

Configure the **array** component within the **sys raid** module using the syntax in the following sections.

Modify

```
modify array [name] [ [add | remove] [hard disk name] ]
```

Display

```
show array
show array [name]
    field-fmt
```

Description

You can use the **array** component to add a hard disk to or remove a hard disk from an array of disks, or to display information about an array of disks.

Examples

show array

Displays information about all of the arrays that are configured on the system.

modify array MD1 remove HD2

Removes hard disk, **HD2** from array, **MD1**.

Options

- **hard disk name**
  Specifies the name of the hard disk that you want to add to or remove from the array. This option is required for the command **modify**.
- **name**
  Specifies the name of the array. This option is required for the command **modify**.

See Also

modify, *show*, *tmsh*

bay

Manages a BIG-IP® system disk drive bay.

Syntax

Manage the **bay** component within the **sys raid** module using the syntax in the following sections.

Modify

```
modify bay [1 | 2]
    flash-led
    no-flash-led
```

Display

```
show bay [1 | 2]
    field-fmt
```

Description

You can use the **bay** component to display information about a system bay, signal the LED on a bay to flash, or signal the LED on a bay to stop flashing. The LED is helpful for identifying the location of a specific disk, see **sys raid disk**.

Examples

modify bay 1 flash-led

Signal the system to make the LED on bay 1 flash.

show bay

Displays information about the system bay.

show bay field-fmt

Displays information about the system bay in a field format.

Options

- **flash-led**
  Signal the LED on the bay to flash.
- **no-flash-led**
  Signal the LED on the bay to stop flashing.

For information about the **field-fmt** option, see **help show**.

See Also

show, *disk*, *tmsh*

disk

Displays information about the BIG-IP® system disks.

Syntax

Display information about the **disk** component within the **sys raid** module using the syntax in the following sections.

Display

```
show disk [name]
    field-fmt
    all-properties
```

Description

You can use the **disk** component to display information about the system disks including name, serial number, and whether the disk is a member of an array of disks. When "all-properties" option is specified, the media wear-out information of the disk is also shown. This include the wear-out indicator, space available, power-on hours, and estimated remaining life.

Examples

show disk

Displays information about all of the system disks.

show disk HD1 field-fmt

Displays information, in a field format, about disk, **HD1**.

show disk SSD1 all-properties

Displays all information (including the media wear-out information) about disk, **SSD1**.

Options

- **name**
  Specifies the name of the disk for which you want to display information.

See Also

show, *tmsh*

104

sys sflow

- Introducing the sys sflow module
- Alphabetical list of components

Introducing the sys sflow module

You can use the tmsh components that reside within the sys sflow module to configure sFlow receivers on the BIG-IP® system. For more information about the tmsh hierarchical structure, see Chapter 2, *Understanding and Using the Traffic Management Shell*.

Alphabetical list of components

The remainder of this chapter lists the tmsh components that are available in the sys sflow module.

receiver

Manages sFlow receivers configured on the BIG-IP system.

Syntax

Configure the **receiver** component within the **sys sflow** module using the syntax shown in the following sections.

Create/Modify

```
create receiver [name]
modify receiver [name]
   address [ip address]
   app-service [[string] | none]
   description [string]
   max-datagram-size [integer]
   port [ip port]
   state [disabled | enabled]
```

Display

```
list receiver
list receiver [ [ [name] | [glob] | [regex] ] ... ]
    all-properties
    one-line
```

Delete

```
delete receiver [name]
```

Description

You can use the **receiver** component to create, delete, list, or modify an sFlow receiver object on the BIG-IP system.

◆ Note

You can add an sFlow receiver to the BIG-IP system, only if you are assigned either the Resource Administrator or Administrator user role.

Examples

create receiver my_receiver address 10.10.10.10

Creates an sFlow receiver object named **my_receiver** with an IP address of **10.10.10.10**, where the **port**, **max-datagram-size**, and **state** options are set to default values.

create receiver my_receiver address 10.20.10.20 port 1234 state enabled

Creates an sFlow receiver object named **my_receiver** with an IP address of **10.20.10.20**, a port of **1234**, and the **max-datagram-size** option set to default value. The state of the receiver is **enabled**.

modify receiver my_receiver state enabled

Changes the state of sFlow receiver object named **my_receiver** to **enabled**.

Options

- **address**
  Specifies the IP address on which the sFlow receiver listens for UDP datagrams. This option is required for the **create** command.
- **app-service**
  Specifies the name of the application service to which the object belongs. The default value is **none**. **Note:** If the **strict-updates** option is **enabled** on the application service that owns the object, you cannot modify or delete the object. Only the application service can modify or delete the object.
- **description**
  User defined description.
- **glob**
  Displays the items that match the glob expression. See **help glob** for a description of **glob** expression syntax.
- **max-datagram-size**
  Specifies the maximum size in bytes of the UDP datagram the sFlow receiver accepts. The default value is **1400**.
- **name**
  Specifies a unique name for the component. This option is required for the commands **create**, **delete**, and **modify**.
- **port**
  Specifies the port on which the sFlow receiver listens for UDP datagrams. The default value is the standard sFlow port, **6343**.
- **regex**
  Displays the items that match the regular expression. The regular expression must be preceded by an at sign (@[regular expression]) to indicate that the identifier is a regular expression. See **help regex** for a description of regular expression syntax.
- **state**
  Specifies the state of the receiver. The sFlow samples will be collected and sent to the receiver when **enabled**. The default value is **disabled**.

See Also

create, *delete*, glob, *list*, *modify*, regex, *tmsh*

105

sys sflow data-source

- Introducing the sys sflow data-source module
- Alphabetical list of components

Introducing the sys sflow data-source module

You can use the tmsh components that reside within the sys sflow datasource module to configure sFlow data sources for the BIG-IP® system. For more information about the tmsh hierarchical structure, see Chapter 2, *Understanding and Using the Traffic Management Shell*.

Alphabetical list of components

The remainder of this chapter lists the tmsh components that are available in the sys sflow data-source module.

http

Displays the status of all HTTP sFlow data sources on the BIG-IP system.

Syntax

Display the status of **http** component within the **sys sflow data-source** module using the syntax shown in the following sections.

Display

```
show http
    all-properties
    field-fmt
```

Description

You can use the **http** component to display the current status of all HTTP sFlow data sources on the BIG-IP system.

Examples

show http

Displays the current status of all HTTP sFlow data sources.

See Also

show, *tmsh*

interface

Displays the status of all sFlow data sources (interfaces) on the BIG-IP system.

Syntax

Display the status of **interface** component within the **sys sflow data-source** module using the syntax shown in the following sections.

Display

```
show interface
    all-properties
    field-fmt
```

Description

You can use the **interface** component to display the current status of all sFlow data sources (interfaces) on the BIG-IP system.

Examples

show interface

Displays the current status of all sFlow data sources (interfaces).

See Also

show, *tmsh*

system

Displays the status of the system sFlow data sources on the BIG-IP system.

Syntax

Display the status of **system** component within the **sys sflow data-source** module using the syntax shown in the following sections.

Display

```
show system
    all-properties
    field-fmt
```

Description

You can use the **system** component to display the current status of the system sFlow data sources on the BIG-IP system.

Examples

show system

Displays the current status of the system sFlow data sources.

See Also

show, *tmsh*

vlan

Displays the status of all sFlow data sources (VLANs) on the BIG-IP system.

Syntax

Display the status of **vlan** component within the **sys sflow data-source** module using the syntax shown in the following sections.

Display

```
show vlan
    all-properties
    field-fmt
```

Description

You can use the **vlan** component to display the current status of all sFlow data sources (VLANs) on the BIG-IP system.

Examples

show vlan

Displays the current status of all sFlow data sources (VLANs).

See Also

show, *tmsh*

106

sys sflow global-settings

- Introducing the sys sflow global-settings module
- Alphabetical list of components

Introducing the sys sflow global-settings module

You can use the tmsh components that reside within the sys sflow global-settings module to configure global sFlow settings on the BIG-IP® system. For more information about the tmsh hierarchical structure, see Chapter 2, *Understanding and Using the Traffic Management Shell*.

Alphabetical list of components

The remainder of this chapter lists the tmsh components that are available in the sys sflow global-settings module.

http

Manages the global HTTP sFlow configuration on the BIG-IP system.

Syntax

Configure the **http** component within the **sys sflow global-settings** module using the syntax shown in the following sections.

Modify

```
modify http
   description [string]
   poll-interval [integer]
   sampling-rate [integer]
```

Display

```
list http
    all-properties
    non-default-properties
    one-line
```

Description

You can use the **http** component to modify or list the global HTTP sFlow configuration on the BIG-IP system.

◆ Note

You can modify the global HTTP sFlow configuration on the BIG-IP system, only if you are assigned either the Resource Administrator or Administrator user role.

Examples

modify http poll-interval 60 sampling-rate 1500

Sets the **poll-interval** to **60** seconds and the **sampling-rate** to **1500** packets for all monitored HTTP data sources on the BIG-IP system.

Options

- **description**
  User defined description.

- **poll-interval**
  Specifies the maximum interval in seconds between polling by the sFlow agent of all monitored HTTP data sources on the BIG-IP system. The default value is **10**.
- **sampling-rate**
  Specifies the ratio of packets observed at all HTTP data sources to the samples generated. For example, a sampling rate of 2000 specifies that 1 sample will be randomly generated for every 2000 packets observed. The default value is **1024**.

See Also

list, *modify*, *tmsh*

interface

Manages the global sFlow configuration for interfaces on the BIG-IP system.

Syntax

Configure the **interface** component within the **sys sflow global-settings** module using the syntax shown in the following sections.

Modify

```
modify interface
   description [string]
   poll-interval [integer]
```

Display

```
list interface
    all-properties
    non-default-properties
    one-line
```

Description

You can use the **interface** component to modify or list the global sFlow configuration for interfaces on the BIG-IP system.

◆ Note

You can modify the global sFlow configuration for interfaces on the BIG-IP system, only if you are assigned either the Resource Administrator or Administrator user role.

Examples

modify interface poll-interval 60

Sets the **poll-interval** to **60** seconds for all monitored data sources (interfaces) on the BIG-IP system.

Options

- **description**
  User defined description.

- **poll-interval**
  Specifies the maximum interval in seconds between polling by the sFlow agent of all monitored data sources (interfaces) on the BIG-IP system. The default value is **10**.

See Also

list, *modify*, *tmsh*

system

Manages the global system sFlow configuration on the BIG-IP system.

Syntax

Configure the **system** component within the **sys sflow global-settings** module using the syntax shown in the following sections.

Modify

```
modify system
   description [string]
   poll-interval [integer]
```

Display

```
list system
    all-properties
    non-default-properties
    one-line
```

Description

You can use the **system** component to modify or list the global system sFlow configuration on the BIG-IP system.

◆ Note

You can modify the global system sFlow configuration on the BIG-IP system, only if you are assigned either the Resource Administrator or Administrator user role.

Examples

modify system poll-interval 60

Sets the **poll-interval** to **60** seconds for the system data sources on the BIG-IP system.

Options

- **description**
  User defined description.

- **poll-interval**
  Specifies the maximum interval in seconds between polling by the sFlow agent of the system data sources on the BIG-IP system. The default value is **10**.

See Also

list, *modify*, *tmsh*

vlan

Manages the global sFlow configuration for VLANs on the BIG-IP system.

Syntax

Configure the **vlan** component within the **sys sflow global-settings** module using the syntax shown in the following sections.

Modify

```
modify vlan
   description [string]
   poll-interval [integer]
   sampling-rate [integer]
```

Display

```
list vlan
    all-properties
    non-default-properties
    one-line
```

Description

You can use the **vlan** component to modify or list the global sFlow configuration for VLANs on the BIG-IP system.

◆ Note

You can modify the global sFlow configuration for VLANs on the BIG-IP system, only if you are assigned either the Resource Administrator or Administrator user role.

Examples

modify vlan poll-interval 60 sampling-rate 1500

Sets the **poll-interval** to **60** seconds and the **sampling-rate** to **1500** packets for all monitored data sources (VLANs) on the BIG-IP system.

Options

- **description**
  User defined description.

- **poll-interval**
  Specifies the maximum interval in seconds between polling by the sFlow agent of all monitored data sources (VLANs) on the BIG-IP system. The default value is **10**.
- **sampling-rate**
  Specifies the ratio of packets observed at all data sources (VLANs) to the samples generated. For example, a sampling rate of 2000 specifies that 1 sample will be randomly generated for every 2000 packets observed. The default value is **2048**.

See Also

list, *modify*, *tmsh*

107

sys software

- Introducing the sys software module
- Alphabetical list of components

Introducing the sys software module

You can use the tmsh components that reside within the sys software module to configure the BIG-IP® system settings and display information about the system. For more information about the tmsh hierarchical structure, see Chapter 2, *Understanding and Using the Traffic Management Shell*.

Alphabetical list of components

The remainder of this chapter lists the tmsh components that are available in the sys software module.

block-device-image

Manages F5 Networks block device software images.

Syntax

Install, display information about, using the syntax in the following sections.

Install

```
install
    create-volume
    image [name]
    reboot
    volume [name]
```

Display

```
list block-device-image
list block-device-image [ [ [ name [/slot_id] ] | [glob] | [regex] ] ... ]
    build
    build-date
    checksum
    device-agent
    file-size
    last-modified
    one-line
    product
    resource-id
    verified
    version
```

Description

You can use the **block-device-image** component to install images from block devices onto a volume, or view information about available block-device-images.

Installing A Software Block-Device-Image

Before you begin installing a block-device-image, the image must be be made available to the system. As of this writing, block device images are only available from within a VCMP guest via a virtual cdrom service. A VCMP host administrator must have provided the images for use by the guest as part of there administration of the VCMP host.

From tmsh, you can use **show sys software status** to see all of the available disk volumes where you can install the image. You can install the image file in any volume that is not active.

Then use the **install** command with this component to install the image to an unused volume. You can use the **create-volume** option if you want to create a new volume. The installation takes some time; you can use **show sys software status** repetitively to watch the progress of the installation. To put the newly installed software into active service, use the **reboot** option in the **install** command, or use the **reboot volume** *vol-name* command after the **install** command completes.

◆ Note

*You use the **slot_id** option only for chassis systems and only when displaying the values for the options of a specific block-device-image. You do not use the **slot_id** option when installing or deleting an block-device-image, because these commands operate on all blades or the entire system.*

Confirming An Block-Device-Image Installation

You can use **show sys version** to confirm that the system is running the new software version. If this is a new module for the current system, you may need to use **show sys license** and/or **install sys license** to update your license. For a new module, you may also need to provision CPU, memory, and disk space for the module with the **sys provision** component.

Examples

install block-device-image BIGIP-10.0.0.5376.0.iso volume HD1.1 reboot

Attempts to install the specified block-device-image, **BIGIP-10.0.0.5376.0.iso**, onto **HD1.1**. **Note:** If the installation is successful, the machine reboots into the newly installed block-device-image.

list block-device-image BIGIP-10.0.0.5376.0.iso

Displays information about the specified block-device-image, **build 5376.0 of BIG-IP version 10.0.0**.

list block-device-image */1

Displays information about all of the block-device-images located on the first slot.

Options

- **build**
  Displays the build number of the block-device-image.
- **build-date**
  Displays the date on which the block-device-image was built.
- **checksum**
  Displays the checksum of the block-device-image. You can use this option to verify the integrity of the block-device-image.

- **create-volume**
  Creates a new volume using the name specified with the **volume** option. Mirrored volume names must begin with the prefix **MD1.**. Mirrored volumes are available only on systems that support RAID, see **sys raid**.
- **device-agent**
  Displays the name of the service which is repsonsible for managing the type of block device on which a give image is available.
  vcmp-virtual-cdrom is the **device-agent** which allows VCMP guests to install images that reside in the host system, via a virtual cdrom device.
- **file-size**
  Displays the size of the block-device-image file in megabytes.
- **glob**
  Displays the items that match the **glob** expression. See **help glob** for a description of **glob** expression syntax.
- **last-modified**
  Displays the date the file was last modified.
- **name**
  Specifies the name of the block-device-image that you want to install or delete.
- **product**
  Displays the F5 Networks product the block-device-image contains.
- **reboot**
  Specifies that the system reboots immediately after a successful installation.
- **regex**
  Displays the items that match the regular expression. The regular expression must be preceded by an at sign (@[regular expression]) to indicate that the identifier is a regular expression. See **help regex** for a description of regular expression syntax.
- **resource-id**
  Displays the resource-id string corresponding to software image in question. This string is used to identify the image for use in interacting with the device agent that is responsible for management of the resource. In the case of the **vcmp-virtual-cdrom device-agent** the resource-id is used by the live installation daemon when requesting that the hypervisor make images available, before the installation can proceed.
- **verified**
  When set to **yes**, indicates that the block-device-image is authentic.
- **version**
  Displays the version number of the product this block-device-image contains.

- **volume**
  Specifies the name of the volume on which you want to install the block-device-image, or from which you want to delete the block-device-image.

◆ Note

You cannot install software on the active volume.

See Also

delete, glob, *install*, *list*, *reboot*, regex, sys software block-device-hotfix, *hotfix*, *image*, *tmsh*, *show*, *status*, *version*, *license*, *provision*

block-device-software-hotfix

Manages F5 Networks block device software hotfixes.

Syntax

Install, or display information about using the syntax in the following sections.

Install

```
install block-device-hotfix [name] volume [name]
    create-volume
    reboot
```

Display

```
list block-device-hotfix
list block-device-hotfix [ [ [ name [/slot_id] ] | [glob] | [regex] ] ... ]
    build
    checksum
    device-agent
    id
    one-line
    product
    title
    resource-id
    verified
    version
```

Description

You can use the **block-device-hotfix** component to install a block-device-hotfix onto a volume, or view information about available block-device-hotfixes.

Use the **create-volume** option with the **block-device-hotfix** component to create new volumes.

◆ Note

*You use the **slot_id** option only for chassis systems and only when displaying the values for the options of a specific block-device-hotfix. You do not use the **slot_id** option when installing or deleting a block-device-hotfix, because these commands operate on all blades or the entire system.*

Examples

list block-device-hotfix Hotfix-BIGIP-9.6.1-824.0-HF3.im

Displays information about the specified block-device-hotfix, **BIGIP-9.6.1-824.0-HF3.im**.

list block-device-hotfix */1

Displays information about the all the block-device-hotfixes on the first slot.

install block-device-hotfix Hotfix-BIGIP-9.6.1-824.0-HF3.im volume HD1.1 reboot

Attempts to install the specified block-device-hotfix, **BIGIP-9.6.1-824.0-HF3.im**, onto **HD1.1**.

◆ Note

*If the installation is successful, and you used the **reboot** option, as in this example, the machine reboots into the newly installed block-device-hotfix.*

Options

- **build**
  Displays the build number of the block-device-hotfix.
- **checksum**
  Displays the checksum of the block-device-hotfix.
- **create-volume**
  Create a new volume using the name specified with the **volume** option. Mirrored volume names must begin with the prefix **MD1.**. Mirrored volumes are available only on systems that support RAID, see **sys raid**.
- **device-agent**
  Displays the name of the service which is repsonsible for managing the type of block device on which a give hotfix is available. **vcmp-virtual-cdrom** is the **device-agent** which allows VCMP guests to install hotfixes that reside in the host system, via a virtual cdrom device.
- **glob**
  Displays the items that match the **glob** expression. See **help glob** for a description of **glob** expression syntax.
- **name**
  Specifies the name and sequential ID of the block-device-hotfix that you want to install or delete.
- **product**
  Displays the F5 Networks product this block-device-hotfix contains.
- **reboot**
  Specifies that the system reboots immediately after a successful installation.
- **resource-id**
  Displays the resource-id string corresponding to software **block-device-hotfix** in question. This string is used to identify the image for use in interacting with the device agent that is responsible for management of the resource. In the case of the **vcmp-virtual-cdrom**

device-agent the resource-id is used by the live installation daemon when requesting that the hypervisor make hotfixes available before the installation can proceed.

- **regex**
  Displays the items that match the regular expression. The regular expression must be preceded by an at sign (@[regular expression]) to indicate that the identifier is a regular expression. See **help regex** for a description of regular expression syntax.
- **slot_id**
  Specifies the number of the slot on a chassis system that contains the block-device-hotfix about which you want to display information.
- **title**
  Displays a textual description of the block-device-hotfix.
- **verified**
  When set to **yes**, indicates that the block-device-hotfix is authentic.
- **version**
  Displays the version number of the product the block-device-hotfix contains.
- **volume**
  Specifies the name of the volume on which you want to install the block-device-hotfix, or from which you want to delete the block-device-hotfix.

See Also

delete, glob, *install*, *list*, regex, *block-device-image*, *hotfix*, *image*, *tmsh*

hotfix

Manages F5 Networks software hotfixes.

Syntax

Install, display information about, or delete a hotfix using the syntax in the following sections.

Install

```
install hotfix [name] volume [name]
    create-volume
    reboot
```

Display

```
list hotfix
list hotfix [ [ [ name [/slot_id] ] | [glob] | [regex] ] ... ]
    build
    checksum
    id
    one-line
    product
    title
    verified
    version
```

Delete

```
delete hotfix [ [name] ... ]
    all
```

Description

You can use the **hotfix** component to install a hotfix onto a volume, view information about available hotfixes, or delete unwanted hotfixes.

Use the **create-volume** option with the **hotfix** component to create new volumes.

◆ Note

*You use the **slot_id** option only for chassis systems and only when displaying the values for the options of a specific hotfix. You do not use the **slot_id** option when installing or deleting a hotfix, because these commands operate on all blades or the entire system.*

Examples

list hotfix Hotfix-BIGIP-9.6.1-824.0-HF3.im

Displays information about the specified hotfix, **BIGIP-9.6.1-824.0-HF3.im**.

list hotfix */1

Displays information about the all the hotfixes on the first slot.

install hotfix Hotfix-BIGIP-9.6.1-824.0-HF3.im volume HD1.1 reboot

Attempts to install the specified hotfix, **BIGIP-9.6.1-824.0-HF3.im**, onto **HD1.1**.

◆ Note

*If the installation is successful, and you used the **reboot** option, as in this example, the machine reboots into the newly installed hotfix.*

Options

- **build**
  Displays the build number of the hotfix.
- **checksum**
  Displays the checksum of the hotfix. You can use this option to verify the integrity of the hotfix.
- **create-volume**
  Create a new volume using the name specified with the **volume** option. Mirrored volume names must begin with the prefix **MD1.**. Mirrored volumes are available only on systems that support RAID, see **sys raid**.
- **glob**
  Displays the items that match the **glob** expression. See **help glob** for a description of **glob** expression syntax.
- **name**
  Specifies the name and sequential ID of the hotfix that you want to install or delete.
- **product**
  Displays the F5 Networks product this hotfix contains.
- **reboot**
  Specifies that the system reboots immediately after a successful installation.
- **regex**
  Displays the items that match the regular expression. The regular expression must be preceded by an at sign (@[regular expression]) to indicate that the identifier is a regular expression. See **help regex** for a description of regular expression syntax.
- **slot_id**
  Specifies the number of the slot on a chassis system that contains the hotfix about which you want to display information.

- **title**
  Displays a textual description of the hotfix.
- **verified**
  When set to **yes**, indicates that the hotfix is authentic.
- **version**
  Displays the version number of the product the hotfix contains.
- **volume**
  Specifies the name of the volume on which you want to install the hotfix, or from which you want to delete the hotfix.

See Also

delete, glob, *install*, *list*, regex, *image*, *tmsh*

image

Manages F5 Networks software images.

Syntax

Install, display information about, or delete a software image using the syntax in the following sections.

Install

```
install
    create-volume
    image [name]
    reboot
    volume [name]
```

Display

```
list image
list image [ [ [ name [/slot_id] ] | [glob] | [regex] ] ... ]
    build
    build-date
    checksum
    file-size
    last-modified
    one-line
    product
    verified
    version
```

Delete

```
delete image [ [ [name] ... ] | [all] ]
```

Description

You can use the **image** component to install images onto a volume, view information about available images, or delete unwanted images.

Installing A Software Image

Before you begin installing an image, you must download the image file into the /shared/images directory. You can find new software images at http://downloads.f5.com. We recommend downloading both the .iso file and the .md5 file. Download the file (or files) to your local machine, then transfer it to the /shared/images directory on the BIG-IP®. Use the Manager (GUI) interface to make this transfer, or **quit** tmsh to the Unix command line and use **scp** or a similar Unix command.

If you downloaded the .md5 file, you can use the Unix **md5sum** command to check the MD5 hash of the .iso file, and you can compare it to the contents of the .md5 file. They should match. If they do not, retry the download and/or transfer of the .iso file.

From tmsh, you can use **show sys software status** to see all of the available disk volumes where you can install the .iso file. You can install the .iso file in any volume that is not active.

Then use the **install** command with this component to install the .iso file to an unused volume. You can use the **create-volume** option if you want to create a new volume. The installation takes some time; you can use **show sys software status** repetitively to watch the progress of the installation. To put the .iso file into active service, use the **reboot** option in the **install** command, or use the **reboot volume** *vol-name* command after the **install** command completes.

◆ Note

*You use the **slot_id** option only for chassis systems and only when displaying the values for the options of a specific image. You do not use the **slot_id** option when installing or deleting an image, because these commands operate on all blades or the entire system.*

Confirming An Image Installation

You can use **show sys version** to confirm that the system is running the new software version. If this is a new module for the current system, you may need to use **show sys license** and/or **install sys license** to update your license. For a new module, you may also need to provision CPU, memory, and disk space for the module with the **sys provision** component.

Examples

install image BIGIP-10.0.0.5376.0.iso volume HD1.1 reboot

Attempts to install the specified image, **BIGIP-10.0.0.5376.0.iso**, onto **HD1.1**. **Note:** If the installation is successful, the machine reboots into the newly installed image.

list image BIGIP-10.0.0.5376.0.iso

Displays information about the specified image, **build 5376.0 of BIG-IP version 10.0.0**.

list image */1

Displays information about all of the images located on the first slot.

Options

- **build**
  Displays the build number of the image.

- **build-date**
  Displays the date on which the image was built.
- **checksum**
  Displays the checksum of the image. You can use this option to verify the integrity of the image.
- **create-volume**
  Creates a new volume using the name specified with the **volume** option. Mirrored volume names must begin with the prefix **MD1.**. Mirrored volumes are available only on systems that support RAID, see **sys raid**.
- **file-size**
  Displays the size of the image file in megabytes.
- **glob**
  Displays the items that match the **glob** expression. See **help glob** for a description of **glob** expression syntax.
- **last-modified**
  Displays the date the file was last modified.
- **name**
  Specifies the name of the image that you want to install or delete.
- **product**
  Displays the F5 Networks product the image contains.
- **reboot**
  Specifies that the system reboots immediately after a successful installation.
- **regex**
  Displays the items that match the regular expression. The regular expression must be preceded by an at sign (@[regular expression]) to indicate that the identifier is a regular expression. See **help regex** for a description of regular expression syntax.
- **verified**
  When set to **yes**, indicates that the image is authentic.
- **version**
  Displays the version number of the product this image contains.
- **volume**
  Specifies the name of the volume on which you want to install the image, or from which you want to delete the image.

◆ Note

You cannot install software on the active volume.

See Also

delete, glob, *install*, *list*, *reboot*, regex, *hotfix*, *tmsh*, *show*, *status*, *version*, *license*, *provision*

signature

Manages F5 Networks software signatures.

Syntax

Display information about, or delete a signature using the syntax in the following sections.

Display

```
list signature
list signature [ [ [ name [/slot_id] ] | [glob] | [regex] ] ... ]
    one-line
```

Delete

```
delete signature [ [name] ... ]
    all
```

Description

You can use the **signature** component to view information about available signatures, or delete unwanted signatures.

◆ Note

*You use the **slot_id** option only for chassis systems and only when displaying the values for the options of a specific signature. You do not use the **slot_id** option when deleting a signature, because these commands operate on all blades or the entire system.*

Examples

list signature BIGIP-11.5.0.0.0.135.iso.sig

Displays information about the specified signature, **BIGIP-11.5.0.0.0.135.iso.sig**.

list signature */1

Displays information about the all the signatures on the first slot.

Options

- **regex**
  Displays the items that match the regular expression. The regular expression must be preceded by an at sign (@[regular expression]) to indicate that the identifier is a regular expression. See **help regex** for a description of regular expression syntax.
- **slot_id**
  Specifies the number of the slot on a chassis system that contains the hotfix about which you want to display information.

See Also

delete, glob, *list*, regex, *image*, *tmsh*

status

Displays the status of a BIG-IP® system software installation.

Syntax

Display information about the **status** component within the **sys software** module using the following syntax.

Display

```
show status
    field-fmt
```

Description

You can use the **status** component to display the status of the software installation, including whether the system is active, the name of the product being installed, the software version and build number of the software, and the slot and volume on which the software is installed.

After you use the **install sys software image** command (see *install* and *image*) to install a new software image, you can use this command to monitor the progress of the installation. A percentage meter appears in the **Status** column.

Examples

```
show status
```

Displays the status of the software installation in a table.

```
show status field-fmt
```

Displays the status of the software installation separately for each volume on the system.

```
root@(big-ip1)(cfg-sync Standalone)(Active)(/Common)(tmos)# quit
[root@big-ip1:Active:Standalone] images # watch tmsh show sys software status
```

Launches the Unix **watch** command from the Unix command line. The command produces auto-updating output similar to this:

```
Every 2.0s: tmsh show sys software status                    Thu Oct 18 14:04:04 2012
--------------------------------------------------------------------
Sys::Software Status
Volume  Product  Version      Build  Active                Status
--------------------------------------------------------------------
HD1.1        EM    3.2.0      222.0      no  installing 6.000 pct
HD1.2        EM    3.2.0  150.0.465     yes              complete
HD1.3        EM    3.2.0       67.0      no              complete
```

Where the "installing 6.000 pct" status increases until it eventually changes to "complete." It changes to a specific failure message if there is an issue.

Options

- **field-fmt**
  Specifies to display the software status for each volume in a field format, rather than in a table.

See Also

show, *tmsh*

update

Displays the BIG-IP® update check schedule settings.

Syntax

Display and modify the **update** component within the **sys software** module using the syntax in the following section.

Modify

```
modify update
       auto-check
       frequency
```

Display

```
list update
       all-properties
       one-line
```

Description

You can use the **update** component to display or modify the configuration of the update check feature.

Examples

list update

Displays update check configuration information for the system.

modify update frequency monthly

Modify the frequency of update checks to monthly.

modify update auto-check disabled

Disable the auto update check feature.

Options

- **auto-check**
  Set this to **enabled** in order to turn on the auto update check feature. **disabled** turns the feature off.
- **check-status**
  This read-only field displays the result of the last update check.

- **errors**
  This read-only field displays the number of consecutive errors detected by update checking.
- **frequency**
  The frequency of update checks can be one of **daily**, **weekly**, or **monthly**.

For information about the options that you can use with the command **list**, see **help list**.

See Also

list, *tmsh*

update-status

Displays the BIG-IP® update check results.

Syntax

Display the results of an update check contained in the **update-status** component within the **sys software** module using the syntax in the following section.

Display

```
list update-status
Options:
    all-properties
    one-line
    [update type] (e.g. RELEASE)
```

Description

You can use the **update-status** component to display the results of the update check feature.

Examples

list update-status

Displays all update check information for the system.

list update-status GEOLOC all-properties one-line

Displays all update check information for the GEOLOC update type on one line.

list update-status last-checked-version

Displays the last checked version for all update types.

Options

- **app-service**
  Specifies the name of the application service to which the object belongs. The default value is **none**. **Note:** If the **strict-updates** option is **enabled** on the application service that owns the object, you cannot modify or delete the object. Only the application service can modify or delete the object.
- **available**
  This is the file name of the available update.

- **check-user**
  This is the system user that last executed the update check.
- **label**
  This is the label used when displaying the status on the GUI.
- **last-checked**
  This is the last time this update type was checked.
- **last-checked-auto-mode**
  This is false if the last time this update type was checked was performed manually.
- **last-checked-version**
  This is the version found at the last time this update type was checked.
- **progress-status**
  This is the state of the update check.
- **supplement**
  This is the file name of the supplemental file.
- **url**
  This is the URL linking to the available update.
- **url-supplement**
  This is a URL linking to a file supplemental to the available update.

For information about the options that you can use with the command **list**, see **help list**.

See Also

list, *tmsh*

volume

Manages software volumes on the BIG-IP® system.

Syntax

Delete, reboot into, or display information about a hard drive **volume** using the syntax in the following sections.

Reboot

```
reboot volume [name]
```

Display

```
list volume
list volume [ [ [name].[slot_id] ] | [glob] | [regex] ] ... ]
show running-config
show running-config [ [ [name].[slot_id] ] | [glob] | [regex] ] ... ]
    active
    active-requested
    all-properties
    basebuild
    build
    edition
    media [media] [size] [default-boot-location]
    one-line
    product
    status
    version
```

Delete

```
delete volume [name]
```

Description

You can use the **volume** component to view information about configured volumes, delete unwanted volumes, and reboot the device to a specific volume.

Volumes are created using the **install** command. See **help sys software image** and the option **create-volume**.

Deleting or rebooting into a volume on a VIPRION system affects the entire chassis; therefore, you do not need to specify the slot number.

Examples

list volume */1

Displays the details of all the volumes located on the first slot in a chassis.

delete volume HD1.5

Deletes the volume named **HD1.5**.

reboot volume HD1.1

Boots into volume **HD1.1** if that volume is not already active. If the volume has an image actively being installed on it, the reboot occurs when the installation is complete.

Options

- **active**
  Specifies if this volume is being run.
- **active-requested**
  Specifies if this volume should be **active** once its status is complete. The system associates this setting with either the active volume or the volume that is going to become active when its status is **complete**. If **active-requested** is set on a volume that is not presently active, the system reboots into the volume when the volume status is **complete**. As an example, **install sys software image BIGIP-10.1.0.3341.0.iso volume HD1.2 reboot** will cause **active-requested** to be set on volume HD1.2, and the system will reboot into volume HD1.2 when the installation is complete. This value is read-only.
- **basebuild**
  Displays the build number of either the hotfix presently applied to the system or the original build.
- **build**
  Displays the original build number (before any hotfixes).
- **edition**
  Displays a textual description of the image. You can use this option to specify the hotfix you want to install.
- **media**
  Displays a description of the physical media on which the volume exists. The options are:
  - **media**
    The type of physical device on which the volume exists, for example, hard drive (hd) or compact flash (cf).
  - **size**
    The space on the slot reserved for the volume.
  - **default-boot-location**
    Specifies the volume into which the system boots if the slot resets.
- **name**
  Specifies the name of the volume you are configuring. Volume names are in the format **HDX.Y**, **CFX.Y**, or **MDX.Y**, where **X** is the hard drive index (HDX), compact flash index (CFX), or RAID index (MDX) (on systems that support RAID), and **Y** is the volume number on that drive.
- **product**
  Displays the F5 Networks product that is installed on the volume.

- **reboot**
  Reboots the system into the specified volume.
- **regex**
  Displays the items that match the regular expression. The regular expression must be preceded by an at sign (@[regular expression]) to indicate that the identifier is a regular expression. See **help regex** for a description of regular expression syntax.
- **status**
  Displays the installation status of the volume. The options are complete or installing.
- **version**
  Displays the version number of the software installed on the volume.

See Also

delete, glob, *install*, *list*, *reboot*, regex, *hotfix*, *image*, *sys raid*, *tmsh*

108

sys url-db

- Introducing the sys url-db module
- Alphabetical list of components

Introducing the sys url-db module

You can use the tmsh components that reside within the sys URL DB module to configure the BIG-IP® system settings and display information about the system.

For more information about the tmsh hierarchical structure, see Chapter 2, *Understanding and Using the Traffic Management Shell*.

Alphabetical list of components

The remainder of this chapter lists the tmsh components that are available in the sys url-db module.

download-result

Lists download result for URL Master and RTSU DB.

Syntax

List **download-result** component within the <sys url-db> module using the syntax shown in the following sections.

Display

The download-result consists of the object name (/Common/masterdb or /Common/rtsudb),and version. These objects are created by BIGIP and cannot be modified or deleted.

```
list url-db download-result [masterdb | rtsudb]
    all-properties
    non-default-properties
    one-line
list url-db download-result masterdb
    db-version [integer]
    ret-code 0
list url-db download-result rtsudb
    db-version [integer]
    ret-code 0
```

Description

Lists download result for Master URL database and Real-Time Security Update (RTSU). These objects are created after the first successful download and updated after every download.

Options

- **db-version**
  Specifies database version for URL Master or Real-Time Security Update DB.
- **ret-code**
  Specifies the download result status and always zero now.

See Also

download-schedule url-category

download-schedule

Configures download schedule for URL Master DB.

Syntax

Configure a **download-schedule** component within the <sys url-db> module using the syntax shown in the following sections.

Modify

The download-schedule consists of the object name (/Common/urldb), download start time (start-time), download end time (end-time) and status. You can have only one download schedule and the download occurs daily.

```
modify url-db download-schedule urldb
    start-time [HH::MM]
    end-time [HH::MM]
    download-now [true | false]
    status true | false]
```

Display

```
list url-db download-schedule urldb
    all-properties
    non-default-properties
    one-line
```

Description

Configures download schedule for Master URL database.

Examples

modify download-schedule urldb { start-time 2:00 end-time 4:00 }

Modify the download schedule for Master DB download schedule between 2:00 AM and 4:00 AM. Other downloads such as RTSU (Real-Time Security Update) and ACE (Advanced Classification Engine) DB download occurs at regular intervals.

modify download-schedule urldb { start-time 20:00 end-time 22:00 }

Modify the download schedule for Master DB download schedule between 8:00 PM and 10:00 AM.

modify download-schedule urldb { download-now true }

Master DB Download starts in few minutes after issuing this command. The download-now will be set to false after successful download.

modify download-schedule urldb { status false }

By setting the status flag to false, download (Master and other DB) will not occur any more.

Options

- **download-now**
  Specifies to start download in few minutes and no need to wait for the scheduled window.
- **end-time**
  Shows download end time. Download will start between scheduled start time and end time.
- **start-time**
  Shows download start time. Download will start between scheduled start time and end time.
- **status**
  Shows the download status is enabled. By turning to false, download will not occur.

See Also

download-result url-category

url-category

Configures URL categories for URL classification and filtering

Syntax

Configure a **url-category** component within the <sys url-db> module using the syntax shown in the following sections.

Create/Modify

Each url-category consists of the object name (/Common/Business_and_Economy), a display-name ("Business and Economy") which is a more user-friendly category name, and a category number. The hundreds and thousands of URLs under a url-category are stored in a database. You can create your own url-category (custom category) and you can add more URLs to an existing category (recategorization).

```
create url-db url-category [name]
    display-name [string]
    description [string]
    initial-disposition [integer]
    is-security-category [string]
    parent-cat-number [integer]
    severity-level [integer]
    urls [add | delete | modify | replace-all-with] {
        [string]
    }
modify url-db url-category [name]
    initial-disposition [integer]
    is-security-category [string]
    parent-cat-number [integer]
    severity-level [integer]
    urls [add | delete | modify | replace-all-with] {
        [string]
    }
```

Display

```
list url-category
list url-category [ [ [name] | [glob] | [regex] ] ... ]
    all-properties
    non-default-properties
    one-line
    partition
```

Description

Configures a url-category

NOTE: When you create a new url-category, you must provide a display-name. However, after creation it cannot be changed to another value. The system will provide a cat-number for your newly created url-category. The number is an integer greater than 1900. The url-category you create is considered to be a custom URL category, and so the is-custom flag will be set to true.

NOTE: The only change you can make to a system provided url-category is to add one or more URLs to its list of URLs. This is called recategorization, and the is-recategory flag will be set to true. You need to do this if the URL does not already exist in the database.

Examples

create url-category my-own-url-cat display-name "My Own URL Category" urls add { http://a.url.com http://www.another.url.org }

Creates a new url-category. The new url-category you create is known as a custom category, as opposed to a system provided url-category. In this case, you must specify the display-name and at least one URL.

modify url-category my-own-url initial-disposition 4 parent-category 0

Modify the initial-disposition and parent-category in a customized url-category.

modify url-category Business_and_Economy urls add { http://www.theneomarxist.com }

Modify a system provided url-category by adding a URL to it. This action is called recategorization. The url-category is recategorized.

Options

- **cat-number**
  Shows a unique category number. Custom URL categories have numbers greater than 1900. This is a read-only attribute.
- **description**
  Specifies a unique description for the URL category.
- **display-name**
  Specifies a user-friendly name that describes what the URL category represents. This attribute cannot be changed after creation.
- **initial-disposition**
  Specifies the action to be taken when a certain URL category is not listed in any url-filter.
- **is-custom**
  This flag is set by the system when you create your own URL category. This attribute is read-only.
- **is-security-category**
  This flag is not being used. This attribute is read-only.

- **parent-cat-number**
  Specifies the category number of a parent url-category. 0 denotes no parent.
- **severity-level**
  Specifies the severity level.

See Also

download-result download-schedule and *url-filter*

109

util

- Introducing the util module
- Alphabetical list of components

Introducing the util module

You can use the tmsh components that reside within the util module to run utilities from within the shell. For more information about the tmsh hierarchical structure, see Chapter 2, *Understanding and Using the Traffic Management Shell*.

Alphabetical list of components

The remainder of this chapter lists the tmsh components that are available in the util module.

ccmode

set Common Criteria mode and a subset of configuration defaults required for a Common-Criteria-compliant BIGIP system.

Syntax

```
ccmode
```

Description

Use this command to set a subset of defaults that are required for a Common-Criteria-compliant system.

Run this command ONLY if you are creating a Common-Criteria-compliant BIG-IP system, or have otherwise determined that all of the changes are desirable for your BIG-IP configuration. Note that there are runtime changes triggered by this command.

Running the ccmode command is an essential part of the configuration changes required to configure a BIG-IP system as Common-Criteria-compliant. This command changes the base configuration in several ways, including:

- defining the minimum required password policy
- defining the allowed cipher sets for SSL/TLS
- disabling some features excluded from the evaluation and therefore not permitted to be used in a compliant system
- setting several DB variables, including the Security.CommonCriteria variable, an indicator from which other runtime changes are triggered.

While running this script is essential to creating a Common-Criteria-compliant system, it is not sufficient. Customers wishing to configure compliant systems must consult the configuration Guidance documentation provided when the evaluation is complete, and follow its instructions to completely configure the BIG-IP.

Ths command has no facility for "undoing" the changes it makes. Instead, the administrator must reverse or revise all of the individual commands, reset the DB variables to their defaults, save the new configuration, and restart the BIG-IP.

dnat

command providing reverse and forward mapping for deterministic NAT (DNAT)

Syntax

Run the **dnat** utility from within the **util** module using the following syntax:

```
run util dnat [<options>] [<address>[:<port>]]
```

Description

The **dnat** utility allows the calculation of forward and reverse source address and port mapping for the deterministic mode of **Large Scale NAT**.

Examples

dnat 10.0.0.1 --action forward Shows a list of translation address/port pairs that might be used for a subscriber at 10.0.0.1, using the DNAT states contained in /var/log/ltm.

dnat 173.240.102.139:5678 Performs a reverse mapping back to the subscriber address for the connection from 173.240.102.139:5678, using the DNAT states contained in /var/log/ltm.

dnat --start_time '2012-09-27 06:30:00' --end_time '2012-09-27 12:10:00' 173.240.102.139:5678 Same as the previous example, but only shows the subscriber addresses that used the translation within the specified time range.

dnat --start_time '2012-09-27 06:30:00' --end_time '2012-09-27 12:10:00' --file /var/log/test 173.240.102.139:5678 Same as the previous example, but use the DNAT states contained in /var/log/test

dnat --file /var/log/test Shows summary information, using the DNAT states contained in /var/log/test

dnat --action summary --start_time '2012-09-27 06:30:00' --end_time '2012-09-27 12:10:00'Shows summary information, using the DNAT states within the specified time range.

Options

- **client_addr** or **--client_addr** <ip_address>
  Used to provide the subscriber address for forward mappings (**--action forward**), and the translation address for reverse mappings (**--action reverse**).

- **client_port** or **--client_port** <port>
  Used to provide the subscriber port for forward mappings (**--action forward**), and the translation port for reverse mappings (**--action reverse**).
- **end_time** or **--end_time** <time>
  End time of search range. User can specify the time format via the **--time-format** switch. The time format defaults to ' **YYYY-MM-DD HH:MM:SS**.'
- **start_time** or **--start_time** <time>
  Start time of search range. User can specify the time format via the **--time-format** switch. The time format defaults to ' **YYYY-MM-DD HH:MM:SS**.'
- **--action** <summary|forward|reverse|reverse_addr>
  Specify the action to be taken: **summary**, **forward**, **reverse**, **reverse_addr**. Default: **reverse** when supplied with **client_addr**, **summary** otherwise.
  - **summary**
    Provides summary information on the parsed deterministic NAT configuration snippet.
  - **reverse**
    Returns possible subscriber address for the provided client address and client port (as translation end-point).
  - **forward**
    Returns possible translation end-points for the provided client address (as subscriber address).
  - **reverse_addr**
    Returns possible subscriber addresses for the provided client address (as translation address).
- **--file** /var/log/ltm
  Read DNAT state from file (default: /var/log/ltm)
- **--time_format** <time_fmt>
  Timestamp parse format for --start_time or --end_time (default: ' **%F %T %Z** ', this yields 'YYYY-MM-DD HH:MM:SS', with timezone being optional.)
- **--all**
  Display all entries, even if there are duplicates (default disabled).
- **--version**
  Display version and DAG information.

See Also

run, *tmsh*, date

lsndb

Run the **lsndb** command to view **Large Scale NAT** persistence entries, inbound mappings, client connection counts, and **PCP** mappings.

Syntax

```
run util lsndb <command> <object>
Commands:
del[ete]
list
summary
Objects:
all
client
inbound[-mapping]
pba
pcp
filters
persist[ence]
all
```

Description

The **lsndb** utility allows users to view **LSN** persistence mappings, inbound mappings, PCP mappings, client connection counts and port block entries. Persistence, inbound and PCP mappings can also be deleted using this utility.

Examples

run util lsndb delete all

Delete all **LSN** persistence mappings, inbound mappings and PCP mappings.

run util lsndb del inbound

Delete all **LSN** inbound mappings.

run util lsndb delete pcp

Delete all **PCP** mappings.

run util lsndb delete persist

Delete all **LSN** persistence entries.

run util lsndb list all

Shows all **LSN** persistence mappings, inbound mappings, PCP mappings, client connection counts and port block entries.

run util lsndb list client

Shows all **LSN** client connection counts.
Each line will display the client IP address and the number of connections used
by the client. Connection counts are only available for LSN pools with a non-zero client connection limit.

run util lsndb list inbound

Shows all **LSN** inbound mappings.
Each line will display the translation IP address, the client IP address, the DS-Lite tunnel (if configured) and the age of the mapping.

run util lsndb list pba

Shows all **LSN** port block entries.
Each line will display the client IP address, the port block used and
the time that the entry will persist in the database (**TTL**).

run util lsndb list pcp

Shows all **PCP** mappings.
PCP clients send MAP requests to map their private IP address and port to a public IP address and port. The BIG IP system uses those mappings as NAT entries. Each line will display the client IP address, the external address used and
the age of the mapping.

run util lsndb list filters

Shows all **LSN** filters for inbound mappings.
Each line will display the <LSN> inbound mappings along with filter's remote peer IP address and prefix length.

run util lsndb list persist

Shows all **LSN** persistence entries.
Each line will display the client IP address, the translation address used and the time that the entry will persist in the database (**TTL**).

run util lsndb summary all

Show summary for all **LSN** persistence mappings, inbound mappings and port block entries.

run util lsndb summary inbound

Show summary for all **LSN** inbound mapping entries.

run util lsndb summary pba

Show summary for all **LSN** port block entries.

run util lsndb summary persist

Show summary for all **LSN** persistence entries.

Options

- **delete**
  Delete all objects of the specified type. Client connection counts and port block entries cannot be deleted.

- **list**
  Display all objects of the specified type.
- **summary**
  Display summary information of the specified type.
  Object types are:
  - **all** = all available object types.
  - **client** = LSN client counts (list only).
  - **inbound** = LSN inbound mapping entries.
  - **pba** = LSN port block entries.
  - **pcp** = PCP mappings entries.
  - **persist** = LSN translation persist entries.

See Also

run, *tmsh*

platform_check

Runs platform diagnostics utility

Syntax

Run the **platform_check** utility from within the **util** module using the following syntax:

```
run util platform_check <test suite>
```

Description

The **platform_check** utility runs the diagnostics to verify correct functionality of platform components. This should be used according to supporting documentation provided by F5.

Output is provided on standard output as well as /var/log/platform_check. Running platform_check with the -h argument will produce available argument listing.

Examples

run util platform_check

Runs all appropriate diagnostics for this platform.

run util platform_check disk

Runs only the disk suite of diagnostics.

See Also

run, *tmsh*

sipdb

Run the **sipdb** command to view **SIP** persistence entries.

Syntax

```
run util sipdb <option>
Options:
-h, --help
-v, --verbose
-r, --router <siprouter-profile>
-k, --key <key>
-d, --delete -r, --router <siprouter-profile> -k, --key <key> -t, --type <type> -p,
--ipproto <proto>
```

Description

The **sipdb** utility allows users to view or delete **SIP** persistence entries.

Examples

run util sipdb

Shows all **SIP** persistence entries.
The output displays key, type, originator, destination, timeout, protocol.
The key is prefixed with persistence type i.e. ‘C’ for call-id persistence, ‘S’ for source address persistence, ‘O’ for custom persistence.
The timeout value displayed is in seconds.

run util sipdb -hrun util sipdb --help Shows the help.

run util sipdb -vrun util sipdb --verbose The output displays the destination transport configuration and pool name in addition to the default values.
The transport name is prefixed with the transport transport type, ‘tc:’ for transport config or ‘vs:’ for virtual server

run util sipdb -r /Common/siprouter-profilerun util sipdb --router /Common/siprouter-profile

Shows **SIP** persistence entries for the routing instance ‘siprouter-profile’ parameter.

run util sipdb -k 3-11768@10.10.10.8run util sipdb --key 3-11768@10.10.10.8

Shows the **SIP** persist record for key 3-11768@10.10.10.8.

run util sipdb -d -r /Common/siprouter-profile -k key1 -t C -p UDPrun util sipdb --delete --router /Common/siprouter-profile --key key1 --type C -ipproto UDP

Delete the **SIP** persist record matching key ‘key1’, type ‘C’ (call-ID), ip-proto ‘UDP’ and router profile ‘/Common/siprouter-profile’.
The type value is either ‘C’ for call id persistence, ‘S’ for source address persistence or ‘O’ for custom persistence.
The ipproto value is either UDP or TCP.

See Also

run, *tmsh*

ssh-keyswap

Run the **ssh-keyswap** command to manage SSH keys on the BIG-IP.

Syntax

```
run util ssh-keyswap <option>
Options:
-genkeys
-checklinks
-delkeys
```

Description

The **ssh-keyswap** utility allows users to generate and delete SSH keys, and check that they are linked properly.

Examples

run util ssh-keyswap -genkeys

Create new local SSH keys and update hosts.

run util ssh-keyswap -checklinks

Check symlinks and make sure they are correct.

run util ssh-keyswap -delkeys

Zeroize and delete local SSH keys when CC mode is enabled.

See Also

run, *tmsh*

test-monitor

Runs an external monitor and displays the inputs to and output from the monitor.

Syntax

Run the **test-monitor** utility from within the **util** module using the following syntax:

```
run util test-monitor <monitor-name> address <ip-address> port <port>
```

Description

The **test-monitor** utility runs a single instance of a monitor against the specified **ip-address**: **port**. The utility output shows the environment, command-line arguments, and resulting messages on stdout and stderr.

Internal monitors are not supported.

Examples

run util test-monitor monitorA address 10.10.10.4 port 80

Runs a monitor on the IP address **10.10.10.4** and port **80**.

See Also

run, *tmsh*

tracepath

Runs the tracepath utility from within tmsh.

Module

util

Syntax

Run the tracepath utility from within the util module using the following syntax:

```
run tracepath [arguments]
```

Read about the arguments that are available for the tracepath utility by accessing the help page from within the util module using the following syntax:

```
help tracepath
```

Description

WARNING

When you are building a batch mode transaction in tmsh, if you type the run command, the system runs the specified program immediately. It does not add the run command to the transaction that you are building.

See also

bash, ccmode, dig, domain-tool, fips-card-sync, fips-util, imish, netstat, help, ping ping6, qkview, run, ssldump, tcpdump, tracepath, tracepath6, traceroute, traceroute6, tmsh, vconsole, zebos

tracepath6

Runs the tracepath6 utility from within tmsh.

Module

util

Syntax

Run the tracepat6h utility from within the util module using the following syntax:

```
run tracepath6 [arguments]
```

Read about the arguments that are available for the tracepath6 utility by accessing the help page from within the util module using the following syntax:

```
help tracepath6
```

Description

WARNING

When you are building a batch mode transaction in tmsh, if you type the run command, the system runs the specified program immediately. It does not add the run command to the transaction that you are building.

See also

bash, ccmode, dig, domain-tool, fips-card-sync, fips-util, imish, netstat, help, ping, ping6, qkview, run, ssldump, tcpdump, tracepath, traceroute, traceroute6, tmsh, vconsole, zebos

traceroute

Runs the traceroute utility from within tmsh.

Module

util

Syntax

Run the traceroute utility from within the util module using the following syntax:

```
run traceroute [arguments]
```

Read about the arguments that are available for the traceroute utility by accessing the help page from within the util module using the following syntax:

```
help traceroute
```

Description

WARNING

When you are building a batch mode transaction in tmsh, if you type the run command, the system runs the specified program immediately. It does not add the run command to the transaction that you are building.

See also

bash, ccmode, dig, domain-tool, fips-card-sync, fips-util, imish, netstat, help, ping ping6, qkview, run, ssldump, tcpdump, tracepath, tracepath6, traceroute6, tmsh, vconsole, zebos

traceroute6

Runs the traceroute6 utility from within tmsh.

Module

util

Syntax

Run the traceroute6 utility from within the util module using the following syntax:

```
run traceroute6 [arguments]
```

Read about the arguments that are available for the traceroute6 utility by accessing the help page from within the util module using the following syntax:

```
help traceroute6
```

Description

WARNING

When you are building a batch mode transaction in tmsh, if you type the run command, the system runs the specified program immediately. It does not add the run command to the transaction that you are building.

See also

bash, ccmode, dig, domain-tool, fips-card-sync, fips-util, imish, netstat, help, ping ping6, qkview, run, ssldump, tcpdump, tracepath, tracepath6, traceroute, tmsh, vconsole, zebos

vconsole

Runs the vconsole utility from within tmsh.

Module

util

Syntax

Run the vconsole utility from within the util module using the following syntax:

```
run vconsole [arguments]
```

Read about the arguments that are available for the vconsole utility by accessing the help page from within the util module using the following syntax:

```
help vconsole
```

Description

WARNING

When you are building a batch mode transaction in tmsh, if you type the run command, the system runs the specified program immediately. It does not add the run to the transaction that you are building.

See also

bash, ccmode, dig, fips-card-sync, fips-util, imish, help, ping6, qkview, run, ssldump, tcpdump, tracepath, tracepath6, traceroute, traceroute6, tmsh, vconsole, zebos

zebos

Runs the zebos utility from within tmsh.

Module

util

Syntax

Run the zebos utility from within the util module using the following syntax:

```
run zebos [arguments]
```

Read about the arguments that are available for the zebos utility by accessing the help page from within the util module using the following syntax:

```
help zebos
```

Description

WARNING

When you are building a batch mode transaction in tmsh, if you type the run command, the system runs the specified program immediately. It does not add the run to the transaction that you are building.

See also

bash, ccmode, dig, domain-tool, fips-card-sync, fips-util, imish, help, ping, ping6, qkview, run, ssldump, tcpdump, tracepath, tracepath6, traceroute, traceroute6, tmsh, vconsole

110

vcmp

- Introducing the vcmp module
- Alphabetical list of components

Introducing the vcmp module

You can use the tmsh components that reside within the vcmp module to manage vCMP® guests and virtual disk images. For more information about the tmsh hierarchical structure, see Chapter 2, *Understanding and Using the Traffic Management Shell*.

Alphabetical list of components

The remainder of this chapter lists the tmsh components that are available in the vcmp module.

global

Display global vCMP system statistics.

Syntax

Configure the **global** component within the **vcmp** module using the following syntax.

Display

```
show global
    (default | exa | gig | kil | meg | peta | raw | tera | yotta | zetta)
```

Description

Use the **global** component within the **vcmp** module to display high-level vCMP system statistics on a per-slot basis. These are statistics that are not associated with any particular vCMP guest or virtual-disk.

Examples

show vcmp global

Display all global vCMP system statistics.

Options

For information about the options that you can use with the **show** command, see **help show**.

See Also

tmsh, *show*, *guest*, *virtual-disk*

guest

Configures a cluster of virtual machines (VMs) that run on one or all slots. This cluster is known as a vCMP guest.

Syntax

Configure the **guest** component within the **vcmp** module using the syntax in the following sections.

Create

```
create guest [name]
modify guest [name]
      hostname [hostname]
      app-service [[string] | none]
      initial-hotfix [hoxfix-filename]
      initial-image [image-filename]
      management-gw [ip-address]
      management-ip [ip-address/netmask | ip-address/prefixlen]
      management-network [bridged | isolated]
      slots [integer]
      min-slots [integer]
      allowed-slots {
          [slot ID] ...
      }
      cores-per-slot [integer]
      state [configured | provisioned | deployed]
      virtual-disk [filename]
      vlans [add | delete | replace-all-with] {
          [VLAN name] ...
      }
      capabilities [add | delete | modify | replace-all-with] {
          [capability Id] [ { value [integer] } ]
      }
```

Display

```
list guest
show guest
options:
  all-properties
  status
```

Delete

```
delete guest [name]
```

Description

Manage vCMP guests running on this host.

Examples

list vcmp guest

Lists the current configuration of all guests.

show vcmp guest

Displays detailed information regarding the state and progress of all guests.

show vcmp guest status

Displays the running state of all guests, including each guest's prompt status.

show vcmp guest all-properties

Displays greater detailed statistics and information on all guests.

create vcmp guest my_guest slots 4 min-slots 2 management-ip 192.168.45.12/24 management-gw 192.168.45.254 initial-image BIGIP-11.0.0.2400.0.iso

Creates a guest that should span four slots, but must span at least two, with the given management IP and gateway, and with the image file BIGIP-11.0.0.2400.0.iso, which is used to install TMOS on the guest's virtual disks. By default, this guest is in the **configured** state and has a management network in **Bridged** mode.

modify vcmp guest my_guest state provisioned

Moves the guest into the **provisioned** state, which causes the host to assign the guest to slots, allocate hardware resources to the guest from those slots, and create virtual disks for the guests on those slots.

<modify vcmp guest my_guest state deployed>

Moves the guest into the **deployed** state, which causes the host to start and maintain VMs on each slot that the guest has been assigned to.

modify vcmp guest my_guest state configured

Moves the guest back to the **configured** state, which causes all of its VMs to shut down and the hardware to be deallocated. The guest is unassigned from all slots. The guest's virtual disks will remain on the host.

Options

- **app-service**
  Specifies the name of the application service to which the guest belongs. The default value is **none**. **Note:** If the **strict-updates** option is **enabled** on the application service that owns the object, you cannot modify or delete the guest. Only the application service can modify or delete the guest.
- **hostname**
  Assigns the specified host name to the guest. The host name must be a FQDN. If none is given, the default of "<guest_name>.localdomain" is used. If the guest's name contains characters that are not allowed in a FQDN, then "localhost.localdomain" is used.

This is only a suggested value and may be changed on the guest itself. If the guest ever reverts to the default host name, this suggested host name is used instead of the normal system default.

- **initial-hotfix**
  Specifies which hotfix image to install on newly created virtual disks for this guest. This image is only used when initially creating the virtual disks. After initial creation, the typical live-install process should be used on the guest to manage software upgrades. The image filename must match a verified software image file that exists in the **/shared/images** directory, otherwise the guest will sit in a wait state on any slot that is missing the hotfix image until that image is added.
  This field is required if the guest **state** is **provisioned** or **deployed**, otherwise it can be left blank.
- **initial-image**
  Specifies which software image to install on newly created virtual disks for this guest. This image is only used when initially creating the virtual disks. After initial creation, the typical live-install process should be used on the guest to manage software upgrades. The image filename must match a verified software image file that exists in the **/shared/images** directory, otherwise the guest will sit in a wait state on any slot that is missing the software image until that image is added.
  This field is required if the guest **state** is **provisioned** or **deployed**, otherwise it can be left blank.
- **management-gw**
  Specifies the IP address of the default gateway for the management network. This IP address is only a suggested value and can be changed on the guest itself. If the guest ever reverts to the default management gateway, the suggested gateway is used instead of the normal system default.
  This field is required if the guest's **management-network** is **bridged**, otherwise it can be left blank.
- **management-ip**
  Specifies the management IP address and netmask to assign to the guest. This address floats to the primary slot of the guest.
  This is only a suggested value and can be changed on the guest itself. If the guest ever reverts to the default management IP address, the suggested IP address is used instead of the normal system default.
  This field is required if the guest's **management-network** is **bridged**, otherwise it can be left blank.
- **management-network**
  Specifies the management network mode for this guest. When in **Bridged** mode, the management interfaces on the guest's VMs are bridged to the physical management interfaces on the host blades. This enables the guest to communicate with networks attached to these physical interfaces, the host itself, and other guests in **Bridged** mode. In **Isolated** mode, the management interfaces of the guest's VMs are completely disconnected. The only way to manage such a guest is by connecting to the console on each of the guest's VMs by using the

/usr/bin/vconsole utility or by connecting through a configured self IP on a guest's VLAN.
The default value is **Bridged**.

- **slots**
  Specifies the number of slots to which this guest should be assigned. This number must be greater than zero and no bigger than the cluster size. The host will attempt to assign the guest up to this number of slots.
  Note that this property can be changed while the guest is in any **state**. While in the **configured** state, modifying the **slots** property has no effect, since the guest has not yet been assigned to any slots. While in the **provisioned** state, decreasing this field will cause the guest to be unassigned from enough slots to honor the new value. The host will unassign the guest first from slots that have the most allocated resources. When a guest's **slots** value is increased, the host attempts to assign the guest to as many slots as possible, up to the new **slots** value. This same behavior occurs when modifying the property while the guest is in the **deployed** state, except that running VMs are shut down on any slots that the guest is unassigned from, and new VMs are deployed on any slots to which the guest has been newly assigned.
  The default value is 1.
- **min-slots**
  This field dictates the number of slots that the guest must be assigned to. If at the end of any allocation attempt the guest is not assigned to at least this many slots, the attempt fails and the change that initiated it is reverted. A guest's **min-slots** value cannot be greater than its **slots** value.
  The default value is 1.
- **allowed-slots**
  This list contains those slots that the guest is allowed to be assigned to. When the host determines which slots this guest should be assigned to, only slots in this list will be considered. This is a good way to force guests to be assigned only to particular slots, or, by configuring disjoint **allowed-slots** lists on two guests, that those guests are never assigned to the same slot.
  By default this list includes every available slot in the cluster. This means by default the guest is allowed to be assigned to any slot.
- **cores-per-slot**
  This value dictates how many cores a guest is allocated from each slot that it is assigned to. Possible values are dependent on the type of blades being used in this cluster. Use tab-completion to see a list of possible values on the current system.
  The default **cores-per-slot** value depends on the type of blades being used in this cluster.
- **state**
  Guests are put into the **configured** state by default. In this state, the configuration for the guest exists on the host, but none of the guest's VMs are running and no hardware resources (for example: CPU cores, memory) are allocated to it. When the guest moves to the **provisioned** state, hardware resources are allocated to it, and if not already present, virtual disks are created, and the **initial-image** is installed onto them. In the **deployed** state, the **vcmpd** daemon on the host blades use the

allocated resources to launch the VMs. Note that moving from the **configured** state to the **deployed** state implies the actions that occur in the **provisioned** state. To shut down a guest's VMs without de-allocating its hardware resources, move the guest from the **deployed** state to the **provisioned** state. Moving a guest to the **configured** state causes its hardware resources to be deallocated. This does not cause the guest's virtual disks to be deleted. They persist on disk and are reused when the vCMP moves back to the **provisioned / deployed** states.

- **virtual-disk**
  Specifies the filename of the virtual disk to use for this guest's VMs. If the filename does not end in **.img**, it is appended. When the guest moves to a **state** in which virtual disks need to be provisioned (**provisioned** or **deployed**), a new virtual disk image will be created for the guest with this given filename on each slot that the guest is assigned to and does not already have a virtual disk image. The **initial-image** is used when creating and installing new virtual disk images. If this field is left blank when virtual disk images need to be provisioned for this guest, a default value of "<guest_name>.img" is assigned. If a virtual disk by that name already exists, then an error is thrown. This prevents virtual disks from accidentally being reused by this assigning of default virtual disk filenames.
- **capabilities**
  This list contains the various capability flags and an optional value associated with the guest. The possible capability flags are: **appliance-mode**. The value attribute for **appliance-mode** is currently ignored and may be omitted. The **appliance-mode** capability may be added or removed from a vCMP guest in any **state**.

See Also

create, *delete*, *list*, *modify*, *show*, *tmsh*, *global*, *virtual-disk*

vdisk

Manages the vCMP virtual disks available on this hypervisor.

Syntax

Configure the **vdisk** component within the **vcmp** module using the syntax in the following sections.

Display

```
list vdisk
options:
  all-properties
show vdisk
```

Delete

```
delete vdisk [name]
```

Description

The **vdisk** component is used to list and delete virtual disks that are used by vCMP guests. Virtual disks are automatically created by **vcmpd** when guests move to the **Provisioned** state and do not already have virtual disks attached to them. This is the only way that virtual disks are created. Virtual disks that are not attached to any guest can be deleted. Virtual disks not already in use can be explicitly attached to vCMP guests.

Examples

list vcmp vdisk

Lists all virtual disks currently available.

delete vcmp vdisk my_vdisk

Deletes the virtual disk named **my_vdisk**. Note that this is only valid if the vdisk is not currently attached to any vCMP guest.

See Also

create, *delete*, *list*, *modify*, *tmsh*

virtual-disk

Manages the vCMP virtual disks available on this hypervisor.

Syntax

Configure the **virtual-disk** component within the **vcmp** module using the syntax in the following sections.

Display

```
list virtual-disk
show virtual-disk

options:
  all-properties

show virtual-disk
```

Delete

```
delete virtual-disk [name]
```

Description

The **virtual-disk** component is used to list and delete virtual disks that are used by vCMP guests. Virtual disks are automatically created by **vcmpd** when guests move to the **Provisioned** state and do not already have virtual disks attached to them. This is the only way that virtual disks are created. Virtual disks that are not attached to any guest can be deleted. Virtual disks not already in use can be explicitly attached to vCMP guests.

Examples

list vcmp virtual-disk

Lists all virtual disks currently available.

delete vcmp virtual-disk my_vdisk

Deletes the virtual disk named **my_vdisk**. Note that this is only valid if the virtual-disk is not currently attached to any vCMP guest.

See Also

create, *delete*, *list*, *modify*, *tmsh*

virtual-disk-template

Manages the vCMP virtual disk templates available on this hypervisor.

Syntax

Configure the **virtual-disk-template** component within the **vcmp** module using the syntax in the following sections.

Display

```
list virtual-disk-template
options:
  all-properties
show virtual-disk-template
```

Delete

```
delete virtual-disk-template [name]
```

Description

The **virtual-disk-template** component is used to list and delete virtual disk templates that are used to create new virtual disk images for vCMP guests. Virtual disk templates are automatically created by **vcmpd** when guests move to the **Provisioned** state and a virtual disk template with the version being installed to the guest's virtual disk image doesn't already exist. This is the only way that virtual disk templates are created. Deleting virtual disk templates frees up space but will slow down future virtual disk image installs of that version; the virtual disk template will need to be first re-created.

Examples

list vcmp virtual-disk-template

Lists all virtual disk templates currently available.

delete vcmp virtual-disk-template my_vdisk

Deletes the virtual disk template named **my_vdisk**. Note that this is only valid if the virtual-disk-template is not currently attached to any vCMP guest.

See Also

tmsh vcmp virtual-disk

III

vcmp health

- Introducing the vcmp health module
- Alphabetical list of components

Introducing the vcmp health module

You can use the tmsh components that reside within the vcmp health module to manage vCMP® guests and virtual disk images. For more information about the tmsh hierarchical structure, see Chapter 2, *Understanding and Using the Traffic Management Shell*.

Alphabetical list of components

The remainder of this chapter lists the tmsh components that are available in the vcmp-health module.

ha-status

Display vCMP guest high availability (HA) status.

Syntax

Display guest HA status using the following syntax.

Display

```
show ha-status
```

Description

Use the **ha-status** component within the **vcmp health** module to display HA status information about the vCMP guests deployed on this system. This is similar to running **tmsh show sys ha-status** inside of a guest.

Examples

show vcmp healh ha-status

Display HA status status for all guests.

show vcmp health ha-status my_guest

Display HA status status for a single guest; "my_guest".

Options

For information about the options that you can use with the **show** command, see **help show**.

module-provision

Display vCMP guest module provisioning status.

Syntax

Display guest module provisioning status using the following syntax.

Display

```
show module-provision
```

Description

Use the **module-provision** component within the **vcmp health** module to display module provisioning status information about the vCMP guests deployed on this system. This will show you which modules are provisioned in a guest and at what level.

Examples

show vcmp healh module-provision

Display module provisioning status for all guests.

show vcmp health module-provision my_guest

Display module provisioning status for a single guest; "my_guest".

Options

For information about the options that you can use with the **show** command, see **help show**.

prompt

Display vCMP guest prompt status.

Syntax

Display guest prompt status using the following syntax.

Display

```
show prompt
```

Description

Use the **prompt** component within the **vcmp health** module to display the per-slot command-line prompts for the vCMP guests deployed on this system. These are the same prompts that one would see when logging into a guest via SSH. Example: "bigip.mydomain.com:/S1-green-P:Active:Standalone"

Examples

show vcmp healh prompt

Display prompt status for all guests.

show vcmp health prompt my_guest

Display prompt status for a single guest; "my_guest".

Options

For information about the options that you can use with the **show** command, see **help show**.

software

Display vCMP guest software status.

Syntax

Display guest software status using the following syntax.

Display

```
show software
```

Description

Use the **software** component within the **vcmp health** module to display software status information about the vCMP guests deployed on this system. This is similar to running **tmsh show sys software** inside the guest.

Examples

show vcmp healh software

Display software status for all guests.

show vcmp health software my_guest

Display software status for a single guest; "my_guest".

Options

For information about the options that you can use with the **show** command, see **help show**.

112

wam

- Introducing the wam module
- Alphabetical list of components

Introducing the wam module

You can use the tmsh components that reside within the wam module to configure BIG-IP® WebAccelerator™. For more information about the tmsh hierarchical structure, see Chapter 2, *Understanding and Using the Traffic Management Shell*.

Alphabetical list of components

The remainder of this chapter lists the tmsh components that are available in the wam module.

ad-policy

Configures an ad policy for WebAccelerator for use in ad insertion.

Syntax

Configure the **ad-policy** within the **wam** module using the syntax shown in the following sections.

Create/Modify

```
create ad-policy [name]
modify ad-policy [name]
   ad-insertion-order [random | sequential]
   ads [add | delete | modify] {
       [name] {
          url [url]
          preroll [yes | no]
       }
   }
   description [string]
```

Display

```
list ad-policy [name ...]
```

Delete

```
delete ad-policy [name ...]
```

Description

You can use the **ad-policy** component to manage the WebAccelerator ad policies. An ad policy defines how the ad insertion is to be performed while processing video resources. Individual ad urls can be configured in the ad-policy along with the insertion order.

Examples

create wam ad-policy my_ad_policy ads add { my_ad1 { preroll yes url http://www.example.com/ad1.m3u8 } }

Creates an ad policy named **my_ad_policy** with an ad named **my_ad1** for the url **http://www.example.com/ad1.m3u8** and as a preroll candidate.

list wam ad-policy my_ad_policy

Displays properties of the ad policy named **my_ad_policy**.

delete wam ad-policy my_ad_policy

Deletes the ad policy named **my_ad_policy**.

Options

- **ad-insertion-order**
  Specifies whether the ads are to be inserted randomly or in the order specified in the policy.
- **ads**
  Specifies the collection of ads.
- **description**
  User defined description of an ad policy.

Ad Options

- **url**
  Specifies the url of the ad.
- **preroll**
  Specifies that the ad is a candidate for preroll insertion. Preroll ad is inserted at the beginning of the playist.

See Also

create, *delete*, *edit*, *list*, *modify*, *show*, *tmsh*

application

Configures application for WebAccelerator.

Syntax

Configure the **application** component within the **wam** module using the syntax shown in the following sections.

Create/Modify

```
create application [name]
modify application [name]
   app-service [[string] | none]
   code [number]
   content-expiration-time [date and time]
   description [string]
   hosts [add | delete | modify | replace-all-with] {
     [ [host name] | [glob] ] {
           app-service [[string] | none]
           code [number]
           subdomain-number-of-http [number]
           subdomain-number-of-https [number]
           subdomain-prefix [string]
      }
   }
   ibr-adaptive-lifetime [number]
   ibr-default-lifetime [number]
   ibr-prefix [string]
   info-header [none | standard | debug]
   multibox [disabled | farm | symmetric]
   policy [name]
   perf-monitor [enabled | disabled]
   perf-monitor-data-retention-period [number]
   collect-roi-statistics [ enabled | disabled ]
   send-metadata [never | always | uncompressed]
   roi-report-email-addresses { string }
   roi-report-frequency [ every-month | every-week ]
   roi-report-name [string]
   roi-report-next-time [date and time]
   roi-report-smtp-config [ smtp configuration object name ]
   roi-report-collect-statistics { caching-bytes-saved | client-ibred-links |
       compression-bytes-saved | icc-refed-links | inlined-links |
       caching-requests-saved | client-ibred-links-recd | icc-inlined-links |
       image-opt-bytes-saved | minification-bytes-saved }
edit application [ [ [name] | [glob] | [regex] ] ... ]
    all-properties
    non-default-properties
reset-stats application
reset-stats application [ [ [name] | [glob] | [regex] ] ... ]
```

Display

```
list application [name ...]
show running-config application [name ...]
   all-properties
```

```
   non-default-properties
   partition
   predefined
show application
show application [name]
  all-properties
  (default | exa | gig | kil | meg | peta | raw | tera | yotta | zetta)
  detail
  field-fmt
```

Delete

```
delete application [name ...]
```

◆ Note

You must remove all references to an application before you can delete it.

Description

You can use the **application** component to configure the host map, select policies, and set application wide parameters that affect WebAccelerator behavior.

Examples

create application my_app hosts add { host1.com host2.com } policy my_local_policy

Creates a WebAccelerator application with a host map consisting of two hosts, **host1.com** and **host2.com**, and a local policy set to **my_local_policy**.

modify application my_app remote-policy my_remote_policy

Sets **my_remote_policy** as the remote policy for application **my_app**.

modify application my_app modify hosts { host1.com { subdomain-number-of-http 3 subdomain-prefix abcd } }

Sets the number of subdomain hosts to 3 and the subdomain prefix to **abcd**for host **host1.com** of WebAccelerator application **my_app**.

modify application my_app roi-report-name "my_report" roi-report-frequency monthly roi-report-next-time now roi-report-email-addresses add { someone@domain.com } roi-report-smtp-config smtp-config roi-report-collect-statistics add { caching_bytes_saved caching_requests_saved }

Sets the ROI report name to my_report. The ROI report is set to be sent monthly, and the next time to send the report is set to now. The ROI report will be mailed to someone@domain.com. The SMTP configuration used to send the ROI report will be the predefined configuration of name

smtp-config. The ROI report will contain the statistics specified by roi-report-collect-statistics, which in this case would be caching_bytes_saved and caching_requests_saved.

delete application my_app

Deletes WebAccelerator application **my_app**.

Options

- **app-service**
  Specifies the name of the application service to which the object belongs. The default value is **none**. **Note:** If the **strict-updates** option is **enabled** on the application service that owns the object, you cannot modify or delete the object. Only the application service can modify or delete the object.
- **code**
  Specifies a numeric non-zero code of the application or application host, which is used for troubleshooting and performance reporting. Each application or application host must have a unique code. If not supplied, it will be generated by the system. Use the keyword **generate** to specify that the system generate a new unique code.
- **content-expiration-time**
  Specifies the date and time that limits how old cached documents can be to still be served from the cache. All documents older than this date and time are considered expired. For example, the following example expires all cached documents of the application **my_app**:
  modify application my_app content-expiration-time now
- **description**
  Specifies the object type description.
- **hosts**
  Specifies the list of domain names (host names) that might appear in HTTP requests for your Web application. These are the same host names that DNS has mapped to the server machine on which your WebAccelerator system is running. To map a group or range of requested host names to a single destination host, you can use an asterisk (*) as a wildcard for the first part of the host name.
- **ibr-adaptive-lifetime**
  Specifies the adaptive lifetime for Intelligent Browser Referencing in seconds. The default value is **864000** (10 days).
- **ibr-default-lifetime**
  Specifies the lifetime for Intelligent Browser Referencing in seconds. The default value is **15724800** (6 months).
- **ibr-prefix**
  Specifies a prefix for the Intelligent Browser Referencing tag. The default value is **";wa"**.

- **info-header**
  Enables and controls the appearance of HTTP header **X-WA-Info:** in responses from WebAccelerator. This header can be used for troubleshooting the WebAccelerator system and for tuning policies. The possible values are:
  - **debug**
    HTTP header **X-WA-Info:** is included into responses with standard information, with some additional values to aid WebAccelerator troubleshooting.
  - **none**
    HTTP header **X-WA-Info:** is not included into responses.
  - **standard**
    HTTP header **X-WA-Info:** is included into responses with standard information, such as S-code, policy, and node codes, etc.
  -

- **multibox**
  Specifies which type of multibox support is required for this application, if any. Options are **disabled**, for deployments with an independent WebAccelerator; **farm**, for farm deployments; and **symmetric**, for symmetric deployments. When this is not **disabled**, the application should be shared by a config sync device group containing all devices in the deployment. It enables the broadcast of invalidation messages to other devices in the device group, and, when set to **symmetric**, also enables symmetric processing of traffic.
- **partition**
  Displays the administrative partition within which the application resides.
- **perf-monitor**
  Specifies whether performance monitoring for this application is enabled. Enabling performance monitoring on many applications may affect the overall performance of WebAccelerator. The default value is **disabled**.
- **perf-monitor-data-retention-period**
  Specifies the time period in days for how long the performance data must be preserved. The default value is **30** days.
- **collect-roi-statistics**
  Specifies whether ROI statistics collection for this application is enabled. The default value is **disabled**.
- **roi-report-name**
  Specifies the name of ROI statistics report if the statistics collection is enabled and report generation is desired.
- **roi-report-frequency**
  Specifies the frequency of ROI statistics report, if the statistics collection is enabled and report generation is desired. The options are every week or month.

- **roi-report-email-addresses**
  Specifies the email-addresses to which ROI statistics report will be sent.
- **roi-report-next-time**
  Specifies the next time when the ROI statistics report will be sent.
- **roi-report-smtp-config**
  Specifies the smtp configuration that will be used to send the scheduled ROI report over email.
- **roi-report-collect-statistics**
  Specifies which statistics are to be included in the ROI statistics report.
- **policy**
  Specifies the acceleration policy to which you want to assign the new Web application.
- **predefined**
  Displays if this application is predefined.
- **send-metadata**
  Specifies when Etag HTTP headers will be included into responses. The default value is **always**.
  - **always**
    Etag HTTP headers will always be included into responses.
  - **never**
    Etag HTTP headers will not be included into responses.
  - **uncompressed**
    Metadata HTTP headers will be included only if response is uncompressed.
  -
- **subdomain-number-of-http**
  Specifies the number of HTTP subdomains that you want the WebAccelerator system to generate. The WebAccelerator system uses these additional subdomains only on embedded URLs or links that request images or scripts. The default value is **0**.
- **subdomain-number-of-https**
  Specifies the number of HTTPS subdomains that you want the WebAccelerator system to generate. The WebAccelerator system uses these additional subdomains only on embedded URLs or links that request images or scripts. The default value is **0**.
- **subdomain-prefix**
  Specifies the prefix that you want the system to assign to the subdomains. The default value is **wa**.
  For example, if the Requested Host is www.siterequest.com, and you select **2** from the HTTP Subdomains box and type **w** a in the Subdomain Prefix box, the WebAccelerator system changes the domain on qualifying embedded URLs and links to use the following domains:
  - wa1.www.siterequest.com

- wa2.www.siterequest.com
-

◆ Note

You must configure DNS with these entries, and they must map to the same IP address as the base origin server (www.siterequest.com in this example).

See Also

create, *delete*, *edit*, glob, *list*, *modify*, regex, *reset-stats*, *show*, *tmsh*

domain-list

Configures a list of domains for WebAccelerator for use in inserting DNS prefetch tags.

Syntax

Configure the **domain-list** component within the **wam resource** module using the syntax shown in the following sections.

Create/Modify

```
create domain-list [name]
modify domain-list [name]
   app-service [[string] | none]
   description [[string] | none]
   domains
       [add | delete | none| replace-all-with] {
           [string] ...
   }
```

Display

```
list domain-list [name ...]
```

Delete

```
delete domain-list [name ...]
```

Description

You can use the **domain-list** component to manage the domain list resources used by the WebAccelerator DNS prefetching feature. A domain-list must be created, then added to the appropriate domain-lists on a WebAccelerator policy node in order for the domains within the domain list to be inserted into a document.

Examples

create domain-list my_domain_list domains add {example.com example2.com}

Creates a domain list resource for the domains **example.com** and **example2.com** for use
in inserting DNS prefetch tags.

list domain-list my_domain_list

Displays properties of the domain-list resource named **my_domain_list**.

delete domain-list my_domain_list

Deletes the domain-list resource named **my_domain_list**.

Options

- **app-service**
  Specifies the name of the application service to which the object belongs. The default value is **none**. **Note:** If the **strict-updates** option is **enabled** on the application service that owns the object, you cannot modify or delete the object. Only the application service can modify or delete the object.
- **domains**
  Specifies the domains described by the domain list resource.

See Also

create, *delete*, *edit*, *list*, *modify*, *show*, *tmsh*

object-type

Configures object types for WebAccelerator.

Syntax

Configure the **object-type** component within the **wam** module using the syntax shown in the following sections.

Create/Modify

```
create object-type [name]
modify object-type [name]
   app-service [[string] | none]
   code [ [number] | generate]
   compression [disabled | policy-controlled]
   description [string]
   extensions [add | delete | modify | replace-all-with] {
      [document extension]
      ...
   }
   mime-types [add | delete | modify | replace-all-with] {
      [MIME type]
      ...
   }
   symmetric-compression [ disabled | enabled ]
edit object-type [ [ [name] | [glob] | [regex] ] ... ]
    all-properties
    non-default-properties
```

Display

```
list object-type [ [ [name] | [glob] | [regex] ] ... ]
show running-config object-type [ [ [name] | [glob] | [regex] ] ... ]
   all-properties
   non-default-properties
   group
   partition
   predefined
```

Delete

```
delete object-type [name ...]
```

Description

You can use the **object-type** component to manage recognized types of objects. These object types are used to classify documents processed by WebAccelerator. A document can be classified by its file extension or MIME type.

Examples

create object-type documents.abcd extensions add { abc abcd } mime-types add { text/abcd text/x-abcd }

Creates a WebAccelerator object type named **documents.abcd** that includes all documents with extensions .abc or .abcd, and MIME types text/abcd or text/x-abcd.

delete object-type documents.abcd

Deletes the pool named **documents.abcd**.

list object-type documents.abcd

Displays properties of the object-type named **documents.abcd**.

Options

- **app-service**
  Specifies the name of the application service to which the object belongs. The default value is **none**. **Note:** If the **strict-updates** option is **enabled** on the application service that owns the object, you cannot modify or delete the object. Only the application service can modify or delete the object.
- **code**
  Specifies the numeric non-zero code of the object type, which is used troubleshooting and performance reporting. Each object type must have unique code. If not supplied, it will be generated by the system. Use keyword **generate** to have the system generate a new unique code.
- **compression**
  Specifies if this object type supports compression and when it can be enabled. The default value is **disabled**.
  Valid values are:
  - **disabled**
    Never compresses the response. If you use this option, be aware that it overrides any compression setting configured for the assembly rule that the WebAccelerator system matches to the specified object type. You should use this option only if you want the WebAccelerator system to ignore assembly rules for the specified object type.
  - **policy-controlled**
    Specifies that compression is controlled by WebAccelerator **policy**. The compression setting is specified in the assembly rule that the WebAccelerator system matched for this object type. In most cases, you should use this option.
- **description**
  Specifies the object type description.
- **extensions**
  Specifies the extension the WebAccelerator system should find in the file name or Content-Disposition header of the response, in order to match to the specified object type.

- **group**
  Displays the group portion of the name.
- **mime-types**
  Specifies the MIME-types that the WebAccelerator system should find in the Content-Type header of the response, in order to match to the specified object type.
  - **name**
    Specifies a unique name for the component. This option is required for the commands **create**, **delete**, and **modify**. The name of the object type must be in form **group.type** where **group** is used to organize object type based on common usage pattern. for example, documents, binary, pages. The type is used to uniquely identify the object type within a group.
  - **partition**
    Displays the administrative partition within which the object type resides.
  - **regex**
    Displays the items that match the regular expression. The regular expression must be preceded by an at sign (@[regular expression]) to indicate that the identifier is a regular expression. See **help regex** for a description of regular expression syntax.
- **symmetric-compression**
  Specifies whether this object type will be compressed on the WAN link in a symmetric multibox deployment.

See Also

create, *delete*, *edit*, *list*, *modify*, *show*, *tmsh*

policy

Configures an acceleration policy for WebAccelerator.

Syntax

Configure the **policy** component within the **wam** module using the syntax shown in the following sections.

Create/Modify

```
create policy [name]
modify policy [name]
   app-service [[string] | none]
   code [integer]
   copy-from [name]
   description [string]
   nodes [add | delete | modify | replace-all-with] {
      [name] {
         always-proxy [yes | no]
         app-service [[string] | none]
         assembly-compression [enable | disable]
         assembly-compression-ows [enable | disable]
         assembly-concatenation [enable | disable]
         assembly-concatenation-sets [string ] ...
         assembly-css-inlining [enable | disable]
         assembly-css-inlining-urls [string ] ...
         assembly-css-reorder [enable | disable]
         assembly-css-reorder-cache-size [integer]
         assembly-css-reorder-urls [string ] ...
         assembly-dns-prefetch [enable | disable]
         assembly-dns-prefetch-domain-lists [add | delete | replace-all-with] {
               [string] ...
         }
         assembly-dns-prefetch-https-enable [enable | disable]
         assembly-dns-prefetch-https-automatic [enable | disable]
         assembly-ibr [enable | disable]
         assembly-image-inlining [enable | disable]
         assembly-image-inlining-max-size [integer]
         assembly-image-inlining-urls [string ] ...
         assembly-js-inlining [enable | disable]
         assembly-js-inlining-urls [string ] ...
         assembly-js-reorder [enable | disable]
         assembly-js-reorder-cache-size [integer]
         assembly-js-reorder-urls [string ] ...
         assembly-intelligent-client-cache [enable | disable]
         assembly-icc-force [enable | disable]
         assembly-icc-image-max-size [integer]
         assembly-icc-css-inlining-max-size [integer]
         assembly-icc-js-inlining-max-size [integer]
         assembly-icc-max-num-urls [integer]
         assembly-icc-min-client-expiry [integer]
         assembly-minification [enable | disable]
         assembly-multiconnect [enable | disable]
         assembly-on-proxies [enable | disable]
         assembly-pdf-linearization [enable | disable]
         cache-complete-only [enable | disable]
```

```
        cache-first-hit [yes | no]
        cache-mode [memory-and-disk | memory-only]
        cache-priority [low | medium | high]
        cache-stand-in-period [integer]
        code [integer]
        coherency [blade | cluster]
        defaults-from [name]
        description [string]
        jpeg-quality-is-relative [yes | no]
        jpeg-quality [integer]
        jpeg-strip-keeps-copyright [yes | no]
        jpeg-strip-exif [no | yes | if-safe | make-safe]
        jpeg-sampling factor [preserve | 1x1 | 2x1 | 1x2 | 2x2]
        jpeg-progressive-encoding [yes | no]
    jpegxr-quality [integer]
        lifetime-cache-control-extensions
           [add | delete | replace-all-with] {
              [string] ...
        }
        lifetime-cache-control-extensions none
        lifetime-cache-max-age [integer]
        lifetime-honor-ows [yes | no]
        lifetime-honor-ows-values
           [add | delete | replace-all-with] {
              [all-values | no-cache | no-store | no-transform |
              max-age | must-revalidate | private | proxy-revalidate |
              s-maxage] ...
        }
        lifetime-honor-ows-values none
        lifetime-honor-request [yes | no]
        lifetime-honor-request-values
           [add | delete | replace-all-with] {
              [all-values | no-cache | no-store | no-transform |
              max-age | max-stale | min-fresh] ...
        }
        lifetime-honor-request-values none
        lifetime-http-heuristic [percentage]
        lifetime-insert-no-cache [yes | no]
        lifetime-preserve-response [yes | no]
        lifetime-preserve-response-values
           [add | delete | replace-all-with] {
              [all-values | no-cache | no-store | no-transform |
              max-age | must-revalidate | private | proxy-revalidate |
              s-maxage | custom-extension] ...
        }
        lifetime-preserve-response-values none
        lifetime-response-max-age [integer]
        lifetime-response-s-maxage [integer]
        lifetime-stand-in-codes
           [add | delete | replace-all-with] {
              [HTTP response code] ...
        }
        lifetime-stand-in-codes none
        lifetime-use-heuristic [yes | no]
        object-max-size [integer | from-profile]
        object-min-size [integer | from-profile]
    optimize-for-client [yes | no]
        options { [hidden | nodelete | nowrite] ...}
        order [integer]
        response-codes-cached
           [add | delete | replace-all-with] {
              [HTTP response code] ...
```

```
        }
        viewstate-cache [yes | no]
        viewstate-cache-size [integer]
        viewstate-tag [string]
        video-optimization-fast-start [enable | disable]
        video-optimization-max-bitrate [integer]
        video-optimization-insert-ad [enable | disable]
        video-optimization-preroll-ad [enable | disable]
        video-optimization-ad-frequency [integer]
        video-acceleration-ad-policy [string]
webp-quality [integer]
        matching [add | modify | delete | replace-all-with] {
           [host | path | extension | method:[name] |
            query-param:[name] | unnamed-query-param:[name] |
            path-segment:[name] | cookie:[name] |
            user-agent | referrer | protocol | header:[name] |
            client-ip | content-type] {
              app-service [[string] | none]
              arg-alias [string]
              arg-direction [left-to-right | right-to-left]
              arg-name [string]
              arg-ordinal [number]
              description [string]
              value-case-sensitive [yes | no]
              values [add | modify | delete | replace-all-with] {
                 [ [regex] | [string] ] {
                    app-service [[string] | none]
                    can-be-empty [yes | no]
                    can-be-missing [yes | no]
                    invert-match [yes | no]
                 }
              }
              values none
           }
        }
        matching none
        optimize-image [none | to-jpeg | to-gif | to-png | to-tiff]
        png-256-colors [yes | no]
        request-queueing [enable | disable]
        variation [add | modify | delete | replace-all-with] {
           [host | extension | method:[string] |
            query-param:[name] | unnamed-query-param:[name] |
            path-segment:[name] | cookie:[name] |
            user-agent | referrer | protocol | header:[name] |
            client-ip ] {
              app-service [[string] | none]
              arg-alias [string]
              arg-all [yes | no]
              arg-ambiguous-as-unnamed [yes | no]
              arg-direction [left-to-right | right-to-left]
              arg-name [string]
              arg-ordinal [number]
              description [string]
              value-case-sensitive [yes | no]
              values [add | modify | delete | replace-all-with] {
                 [ [regex] | [string] ] {
                    app-service [[string] | none]
                    cache-as [same | different]
                    can-be-empty [yes | no]
                    can-be-missing [yes | no]
                    invert-match [yes | no]
                    match-all [yes | no]
```

```
            }
         }
         values none
      }
   }
   variation none
   [ proxy | proxy-override ]
      [add | modify | delete | replace-all-with] {
      [host | extension | method:[name] |
       query-param:[name] | unnamed-query-param:[name] |
       path-segment:[name] | cookie:[name] |
       user-agent | referrer | protocol | header:[name] |
       client-ip] {
         app-service [[string] | none]
         arg-alias [string]
         arg-direction [left-to-right | right-to-left]
         arg-name [string]
         arg-ordinal [number]
         description [string]
         value-case-sensitive [yes | no]
         values [add | modify | delete | replace-all-with] {
         [ [regex] | [string] ] {
               app-service [[string] | none]
               can-be-empty [yes | no]
               can-be-missing [yes | no]
               invert-match [yes | no]
            }
         }
         values none
      }
   }
   [ proxy | proxy-override ] none
   substitutions [add | modify | delete | replace-all-with] {
      [name] {
         app-service [[string] | none]
         description [string]
         dst-alias [string]
         dst-direction [left-to-right | right-to-left]
         dst-name [string]
         dst-ordinal [number]
         dst-type [query-param | unnamed-query-param | path-segment]
         dst-urls [add | delete | replace-all-with] {
            [URI] ...
         }
         dst-urls none
         src-alias [string]
         src-direction [left-to-right | right-to-left]
         src-name [string]
         src-ordinal [number]
         src-type
           [ randomizer | request-url | query-param |
            unnamed-query-param | path-segment ]
         src-url [absolute | relative]
      }
   }
   substitutions none
   invalidations [add | modify | delete | replace-all-with] {
      [name] {
         active [yes | no]
         app-service [[string] | none]
         broadcast [no | yes]
         description [string]
```

```
                cache-content [add | modify | delete | replace-all-with] {
                 [host | path | extension | method:[name] |
                  query-param:[name] | unnamed-query-param:[name] |
                  path-segment:[name] | cookie:[name] |
                  user-agent | referrer | protocol | header:[name] |
                  client-ip] {
                    app-service [[string] | none]
                    arg-alias [string]
                    arg-direction [left-to-right | right-to-left]
                    arg-name [string]
                    arg-ordinal [number]
                    description [string]
                    value-case-sensitive [yes | no]
                    request-data-alias [string]
                    request-data-direction [left-to-right | right-to-left]
                    request-data-name [string]
                    request-data-ordinal [number]
                    request-data-type
                       [ host | path | extension | method |
                         query-param | unnamed-query-param |
                         path-segment | cookie | user-agent |
                         referrer | protocol | header |
                         client-ip ]
                    values [add | modify | delete | replace-all-with] {
                      [ [regex] | [string] ] {
                        app-service [[string] | none]
                        can-be-empty [yes | no]
                        can-be-missing [yes | no]
                        invert-match [yes | no]
                      }
                    }
                    values none
                }
             }
          }
       }
    }
    partition [name]
    publish-build [integer]
    publish-comment [string]
    published-on [date]
```

◆ Note

*Policies can be created only in the **Drafts** folder. This is required to support publishing functionality. You may create multiple **Drafts** folders, one for each folder where published policies are going to reside.*

Display

```
list policy [name ...]
show running-config policy [name ...]
   all-properties
   non-default-properties
   partition
   predefined
   state
```

Delete

```
delete policy [name ...]
```

Save/Load

```
save policy [name]
load policy [name]
   overwrite
   file [filename]
```

Publish

```
publish policy [name]
   publish-comment [string]
   publish-build [integer]
```

◆ Note

Published policies can be deleted, but cannot be modified. The only way to update a published policy is to edit and then publish its development version.

Description

You can use the **policy** component to manage WebAccelerator acceleration policies. An acceleration policy is a collection of defined rule parameters that dictate how the WebAccelerator system handles HTTP requests and responses. The WebAccelerator system uses two types of rules to manage content: matching rules and acceleration rules. Matching rules are used to classify requests by object type and match the request to a specific acceleration policy. Once matched to an acceleration policy, the WebAccelerator system applies the associated acceleration rules to manage the requests and responses. There are multiple types of acceleration rules: variation, proxy, proxy override, parameter value substitution, and invalidation. The WebAccelerator system ships with several predefined acceleration policies that are optimized for specific Web applications, in addition to several non-application specific policies for general delivery and one for an optional symmetric deployment.

Examples

◆ Note

*For the following examples, the current folder is assumed to be set to **/Common**.*

create policy "Drafts/My Policy"

Creates a new empty policy named **My Policy** in the folder **/Common/Drafts**.

create policy "Drafts/My Policy" copy-from "/Common/Generic Policy - Complete"

Creates a new policy **My Policy** in the folder **/Common/Drafts** by copying standard system policy **/Common/Generic Policy - Complete**.

modify policy "Drafts/My Policy" copy-from "/Common/Generic Policy - Complete"

Modifies the policy **My Policy** by overwriting it with standard system policy **/Common/Generic Policy - Complete**.

modify policy "Drafts/My Policy" nodes add { "My Node" { default-from Site }}

Adds a new node **My Node** as the child node of the node **Site**.

modify policy "Drafts/My Policy" nodes modify { "My Node" { matching add { content-type { values add { pages.other }}}}}

Adds a new matching rule into the node **My Node**. The rule will match content type of the requests to WAM object type **pages.other**.

publish policy "Drafts/My Policy" publish-comment "Added new node My Node"

Publishes the policy **My Policy**.

modify policy "Drafts/My Policy" nodes delete { "My Node" }

Deletes the node **My Node** from the policy **My Policy**.

delete policy "My Policy"

Deletes the policy **My Policy**.

save policy "My Policy" file policy.txt

Saves the policy **My Policy** into the file **/var/local/wam/policy.txt**.

load policy "Drafts/My Policy" overwrite file /tmp/policy.txt

Loads the policy **My Policy** from the file **/tmp/policy.txt** and overwrites the policy if it already exists.

Policy Options

- **app-service**
  Specifies the name of the application service to which the object belongs. The default value is **none**. **Note:** If the **strict-updates** option is **enabled** on the application service that owns the object, you cannot modify or delete the object. Only the application service can modify or delete the object.
- **code**
  Specifies a numeric non-zero code of the policy that is used for troubleshooting and performance reporting. Each policy must have a unique code. If not supplied, it will be generated by the system. Use the keyword **generate** to specify that the system generate a new unique code.
- **copy-from**
  Specifies the name of an existing policy from which to copy all configuration options. If this field is used in the modify command, the

configuration options of the existing policy will be replaced with the new ones. The **code**, **state**, **publish-build**, **publish-comment**, and **published-at** options are not updated.

- **description**
  User defined description of a policy.
- **nodes**
  Specifies the collection of policy nodes. Matching rules and acceleration rules for acceleration policies are organized on the **Policy Tree**, which consists of nodes. The structure of the **Policy Tree** supports a parent-child relationship. This enables you to easily randomize rules. That is, because a leaf node in a **Policy Tree** inherits all the rules from its root node and branch node, you can quickly create multiple leaf nodes that contain the same rule parameters by creating a branch with multiple leaf nodes. If you override or create new rules at the branch node level, the WebAccelerator system reproduces those changes to the associated leaf nodes.
- **partition**
  Displays the administrative partition within which the policy resides.
- **publish-build**
  Specifies the policy build version that was used during policy publishing. If not specified, this number is automatically incremented by the WebAccelerator system.
- **publish-comment**
  Specifies the user supplied comment that describes the changes in the policy that is being published.
- **published-on**
  Specifies the date and time when this policy was last published.
- **file**
  Specifies the file name where the policy is going to be saved or loaded from. If a full path is not specified, it is set to /var/local/wam directory.
- **overwrite**
  Specifies that the policy file for the **save** command or the policy component for the **load** command can be overwritten if it exists.

Node Options

- **always-proxy**
  Specifies that all requests matching this node must be proxied. If it enabled, **proxy** rules are not used, even if configured. **proxy-override** rules still apply.
- **app-service**
  Specifies the name of the application service to which this node belongs. The default value is **none**. **Note:** If the **strict-updates** option is **enabled** on the application service that owns the object, you cannot modify or delete this node. Only the application service can modify or delete this node.

- **assembly-compression**
  Specifies, when enabled, that the WebAccelerator system compresses content for responses, using gzip-encoding. Note that to use this feature, you must set the compress value for the response's object type in the corresponding **object-type** component, and the client must be able to accept gzip-encoded content. The default value is **enabled**.
- **assembly-compression-ows**
  Specifies, when enabled, that the WebAccelerator system requests gzip-encoded or deflate-encoded content from the origin Web server. Note that the origin Web server will comply only if it supports compression, otherwise it will reply with uncompressed content. The default value is **disabled**.
- **assembly-concatenation**
  Specifies, when enabled, that the WebAccelerator system will perform JavaScript/CSS concatenation in HTML documents. The URLs that may be concatenated are specified using the **assembly-concatenation-sets** option. See the WebAccelerator documentation for more details. The default value is **disabled**.
- **assembly-concatenation-sets**
  Specifies the concatenation sets that are active for this node. If a URL in the HTML document that belongs to one of the enabled sets is found, it will transformed with concatenation using the URL of the configured set. This is an ordered set, and if the URL exists in multiple active concatenation sets, the first set specified by this option will be used. See the WebAccelerator documentation for more details.
- **assembly-css-inlining**
  Specifies, when enabled, that the WebAccelerator system will inline CSS URLs in HTML documents. The CSS URLs that may be inlined are specified using the **assembly-css-inlining-urls** option. See the WebAccelerator documentation for more details. The default value is **disabled**.
- **assembly-css-inlining-urls**
  Specifies the CSS URLs that may be inlined.
- **assembly-css-reorder**
  Specifies, when enabled, that the WebAccelerator system will reorder CSS URLs to the HEAD section of HTML documents. The CSS URLs that may be reordered are specified using the **assembly-css-reorder-urls** option. See the WebAccelerator documentation for more details. The default value is **disabled**.
- **assembly-css-reorder-cache-size**
  Specifies the size of the intermediate cache used to store CSS URLs being reordered. Increasing the size of this cache allows more CSS URLs to be reordered. The default value is **8kB**. The maximum value is **8kB**.
- **assembly-css-reorder-urls**
  Specifies the CSS URLs that may be reordered. The URLs must be fully-qualified and whitespace used to separate URLs. The URLs must correspond to WebAccelerator URL resources created by the command **create wam resource url**. See the help for **wam resource url**.

- **assembly-dns-prefetch**
  Specifies, when enabled, that the WebAccelerator system manipulates an HTML document to add DNS prefetch tags at the end of the head. The DNS prefetch tags added are the combined list of domain lists specified in **assembly-dns-prefetch-domain-lists**. DNS prefetch tags will not be inserted in the following conditions: when DNS prefetching is explictly disabled in the document, either by an HTTP header or by a meta-tag in the head of the HTML document; when the connection is served over HTTPS without **assembly-dns-prefetch-https-enable** enabled; or when the connection is to a client browser that does not support DNS prefetching.
  In a document, most browsers will perform DNS prefetching on all domains linked with an HREF. This will speed up performance by having the browser cache possible DNS resolutions before a client clicks on a link, but DNS prefetching cannot automatically occur when a link is created through other means (such as javascript). Inserting DNS prefetch tags addresses this issue.
  The default value is **disabled**.
- **assembly-dns-prefetch-domain-lists**
  Specifies the lists of domains that will be inserted into a document. The domain lists must correspond to WebAccelerator domain list resources created by the command **create wam resource domain-list**. See the help for **wam resource domain-list**.
- **assembly-dns-prefetch-https-enable**
  Specifies, when enabled, that the WebAccelerator system manipulates an HTML document to add DNS prefetch tags at the end of the head when a document is served over HTTPS when the client browser supports DNS prefetching. By default, most browsers that support DNS prefetching will not do any DNS prefetching on pages served over HTTPS. Enabling **assembly-dns-prefetch-https-enable** will insert a meta-header that will turn on DNS prefetching on the page and a meta-header turning of DNS prefetching for the rest of the page. DNS prefetching cannot be turned on for the rest of an HTML document once the meta-header turning of DNS prefetching is reached.
  DNS prefetching is turned off on most browsers serving pages over HTTPS by default as a security measure. DNS prefetching can be used to track which pages are seen over HTTPS by watching the domain resolution requests sent out by the client. According to DNS prefetch standards currently, turning on DNS prefetching on a page will cause all links in the page to have their domains prefetched. This is mitigated by this option with the insertion of an HTTP meta-header turning off DNS prefetching after the DNS tags inserted by the WebAccelerator system. Turning on DNS prefetching for the rest of the page in a request served over HTTPS can be done with the **assembly-dns-prefetch-https-automatic** option.
  The default value is **disabled**.
- **assembly-dns-prefetch-https-automatic**
  Specifies, when enabled, that the WebAccelerator system will not insert a meta-tag into an HTML document served over HTTPS turning off DNS prefetching for the rest of a page. By default, most browsers that support

DNS prefetching will not do any DNS prefetching on pages served over HTTPS. **assembly-dns-prefetch-https-enable** must be enabled for this option to work.
The default value is **disabled**.

- **assembly-ibr**
  Specifies, when enabled, that the WebAccelerator system manipulates the Web browser cache to reduce requests to your site for relatively static content, such as images and style sheet (CSS) files. The default value is **enabled**.
- **assembly-image-inlining**
  Specifies, when enabled, that the WebAccelerator system will inline image URLs in CSS documents. The image URLs that may be inlined are specified using the **assembly-image-inlining-urls** option. See the WebAccelerator documentation for more details. The default value is **disabled**.
- **assembly-image-inlining-max-size**
  Specifies the maximum size of the image that is allowed to be inlined. The default value is **2kB**. The maximum value is **8kB**.
- **assembly-image-inlining-urls**
  Specifies the image URLs that may be inlined.
- **assembly-js-inlining**
  Specifies, when enabled, that the WebAccelerator system will inline JS URLs in HTML documents. The JS URLs that may be inlined are specified using the **assembly-js-inlining-urls** option. See the WebAccelerator documentation for more details. The default value is **disabled**.
- **assembly-js-inlining-urls**
  Specifies the JS URLs that may be inlined.
- **assembly-js-reorder**
  Specifies, when enabled, that the WebAccelerator system will reorder JavaScript URLs to the end of HTML documents. The JavaScript URLs that may be reordered are specified using the **assembly-js-reorder-urls** option. See the WebAccelerator documentation for more details. The default value is **disabled**.
- **assembly-js-reorder-cache-size**
  Specifies the size of the intermediate cache used to store JavaScript URLs being reordered. Increasing the size of this cache allows more JavaScript URLs to be reordered. The default value is **8kB**. The maximum value is **8kB**.
- **assembly-js-reorder-urls**
  Specifies the JavaScript URLs that may be reordered. The URLs must be fully-qualified and whitespace used to separate URLs. The URLs must correspond to WebAccelerator URL resources created by the command **create wam resource url**. See the help for **wam resource url**.
- **assembly-intelligent-client-cache**
  Specifies, when enabled, that the WebAccelerator system will Intelligent Client Cache HTML documents. See the WebAccelerator documentation for more details. The default value is **disabled**.

- **assembly-icc-force**
  Specifies, when enabled, that the WebAccelerator system will Intelligent Client Cache HTML documents, even if the client does not support HTML5 localstorage. See the WebAccelerator documentation for more details. The default value is **disabled**.
- **assembly-icc-image-max-size**
  Specifies the maximum size of the image that is allowed to be inlined as part of Intelligent Client Caching. The default value is **32kB**. The maximum value is **50kB**.
- **assembly-icc-css-max-size**
  Specifies the maximum size of the CSS that is allowed to be inlined as part of Intelligent Client Caching. The default value is **50kB**. The maximum value is **1024kB**.
- **assembly-icc-js-max-size**
  Specifies the maximum size of the JS that is allowed to be inlined as part of Intelligent Client Caching. The default value is **50kB**. The maximum value is **1024kB**.
- **assembly-icc-max-num-urls**
  Specifies the maximum number of links in an HTML document that are allowed to be inlined as part of Intelligent Client Caching. The default value is **10**. The maximum value is **100**.
- **assembly-icc-min-client-expiry**
  Specifies the minimum client expiry of a resource that is allowed to be inlined as part of Intelligent Client Caching. The default value is **2days**.
- **assembly-minification**
  Specifies, when enabled, that the WebAccelerator system will minify JavaScript and CSS.
- **assembly-multiconnect**
  Specifies, when enabled, that the WebAccelerator system modifies embedded URLs with unique sub-domains that prompt the browser to open more persistent connections for each supported protocol (HTTP or HTTPS). To use this feature, you must configure DNS with the additional domains and map those domains to the same IP address as the base origin server. The default value is **enabled**.
- **assembly-on-proxies**
  Specifies, when enabled, that the WebAccelerator system applies the Content Compression and Intelligent Browser Referencing features (if enabled) to content served to clients, even if the content is not served from the WebAccelerator system's cache. Enable this option if you are using the Content Compression or Intelligent Browser Referencing features. The default value is **enabled**.
- **assembly-pdf-linearization**
  Specifies, when enabled, that the WebAccelerator system applies linearization on PDF documents, if the documents match the node matching rules. PDF linearization transforms the document to include the index of the pages in the beginning. This allows Web browsers to load

and show specific pages rather than a whole document. See the WebAccelerator documentation for more details. The default value is **disabled**.

- **optimize-image**
  Specifies whether image optimization should be applied and the format conversion to use. Each of the 4 supported formats (JPEG, PNG, GIF, TIFF) can be converted to any of the others. Images using a capability unique to one format may lose that feature when converted to a format that does not support it. (For example, animated GIFs or multipage-TIFFs will have only the first image when converted to PNG or JPEG). Transparency will be lost when converting from GIF or PNG to JPEG. TIFF is a container for many different image formats so the results will be best-effort and may not list completely.
  A converted image will likely have a different number of bytes after conversion. Some conversions are likely to produce fewer bytes; however, a requested conversion will be done even if it results in more bytes (for consistency). For example, you may want to offer multiple formats of an image without storing them all on a server.
  A correct Content-Type header will be generated for converted images, but HTML files will not be rewritten.
- **optimize-for-client**Specifies whether to allow conversion to a format and/or size which is optimum for the specific client making the request but which, if saved by that client and later sent elsewhere, might not be appropriate.
- **webp-quality**WebP is a "lossy" compression format. This means when you convert an image to a WebP and then convert it back, you will not get back exactly the same image you started with. Compression changes the amount of information stored (and therefore the number of bytes), but not the image dimensions (the number of pixels). The **webp-quality** attribute represents the absolute quality of the WebP produced. Compression (quality) is represented as a number between 1-100 where 1 is minimal quality, but small, and 100 is high-quality, but large. For most images, useful values of quality will be from about 30-70.
- **jpegxr-quality**JPEG-XR is a "lossy" compression format. This means when you convert an image to a JPEG-XR and then convert it back, you will not get back exactly the same image you started with. Compression changes the amount of information stored (and therefore the number of bytes), but not the image dimensions (the number of pixels). The **jpegxr-quality** attribute represents the absolute quality of the JPEG-XR produced. Compression (quality) is represented as a number between 1-100 where 1 is minimal quality, but small, and 100 is high-quality, but large. For most images, useful values of quality will be from about 5-30.
- **jpeg-quality-is-relative**=item **jpeg-quality**
  JPEG is a "lossy" compression format. This means when you convert an image to a JPEG and then convert it back, you will not get back exactly the same image you started with. Compression changes the amount of information stored (and therefore the number of bytes), but not the image

dimensions (the number of pixels). When **jpeg-quality-is-relative** is set to **no**, the **jpeg-quality** attribute represents the absolute quality of the JPEG produced. Compression (quality) is represented as a number between 1-100 where 1 is minimal quality, but small, and 100 is high-quality, but large. For most images, useful values of quality will be from about 30-100. Because information once lost cannot be regained, converting a low-quality JPEG to a higher quality is pointless and image optimization will prevent that (by not changing the original to a higher JPEG quality).
You might be unable to choose a specific absolute quality for JPEG images. When **jpeg-quality-is-relative** is set to **yes**, the relative JPEG quality setting is enabled. In this case, **jpeg-quality** is a percentage (a number between 1-100) that when multiplied by each JPEG's original quality, becomes its optimized quality.

- **jpeg-strip-exif**
  JPEG files have a header (called EXIF) that contains optional data such as a date, time, camera model, exposure settings, and so on. The EXIF header can also contain a color profile, which is required when included. EXIF headers can be small or large. Unless they contain a color profile, they do not affect displaying the image, and so can be removed if the loss of the information they contain is acceptable. There are four options for this setting:
  - **no**
    Leaves any EXIF headers alone.
  - **yes**
    Always strips EXIF headers.
  - **if-safe**
    Only strips EXIF headers if they do not have color profiles (ensures that images display properly).
  - **make-safe**
    Applies the color profile and then strips the EXIF header (typically decreases image file size). Applying a color profile requires additional CPU time.
- **jpeg-strip-keeps-copyright**This setting affects the meaning of **jpeg-strip-exif**. If it is set, stripping the EXIF header will strip everything except the Copyright notice (if one is present).
- **jpeg-sampling-factor**
  Sets the sampling factor to be used when producing JPEG images. The default value is **preserve**, which matches the original file. You can also explicitly specify this option, as it can sometimes improve compression.
- **jpeg-progressive-encoding**
  When enabled, progressive encoding will be used in JPEG images. For large JPEG files, this can improve compression. When this is enabled, it will be applied only if the file is large enough to improve compression.

- **png-256-colors**
  It is often possible to significantly reduce the size of PNG files without changing their appearance very much by reducing the number of colors to 256 optimally selected values. This optimization is enabled when **png-256-colors** is set to **yes**.
- **cache-complete-only**
  Specifies, when enabled, that the WebAccelerator system caches HTML pages only if the HTML code within the page contains begin and end tags. When disabled, the WebAccelerator system reviews HTTP response headers to determine if the information contained on the page is complete. The default value is **enabled**.
- **cache-first-hit**
  Specifies that the first response should be cached according to the policy caching settings. When this is off, the response is cached when more than one request for the document has been seen. Turning this on can reduce cache churn for unpopular documents. The default value is **no**.
- **cache-mode**
  Specifies how where the cached documents will be stored. The default value is **memory-and-disk**. Possible values are:
  - **memory-and-disk**
    The cached documents will be stored in memory or on disk.
  - **memory-only**
    The cached documents will be stored in memory only.
- **cache-priority**
  Specifies the cache admission priority of documents matching the policy node. Documents with high priority are more likely to be admitted into the cache. The default value is **medium**. Possible values are:
  - **low**
    Documents will have low priority.
  - **medium**
    Documents will have medium priority.
  - **high**
    Documents will have high priority.
- **cache-stand-in-period**
  Specifies the amount of time that the WebAccelerator system continues to serve content from cache if the origin Web server does not respond to the WebAccelerator system's requests for fresh content. The default value is **0** (zero), which means the WebAccelerator system responds to requests for expired content with a HTTP 404 error.
- **code**
  Specifies a numeric non-zero code for the node that is used for troubleshooting and performance reporting. All nodes must have unique codes within the policy. If not supplied, the code will be generated by the system. Use the keyword **generate** to specify that the system generate a new unique code.

- **coherency**
  Specifies if the WebAccelerator system will attempt to keep content matching the associated node in sync across the blades of a cluster. The default behavior is to keep content in sync.
  - **blade**
    The cached documents will not be kept coherent across blades. This causes each blade to have its own copy of a given cached document.
  - **cluster**
    The cached documents will be kept coherent across blades. This causes the cluster to have single version of a given cached document.
- **defaults-from**
  Specifies the node that you want to use as the parent node. Your new node inherits all options and values from the parent node specified. The default value is **none**, which means this is a root node.
- **description**
  User defined description of a node.
- **invalidations**
  Specifies the collection of invalidations rules. Invalidations rules enable you to expire cached content before it has reached its time-to-live (TTL) value. This is useful when content updates are event-driven, such as when an item is added to a shopping cart, a request contains a new auction bid, or a poster has submitted content on a forum thread. Invalidations rules can be created only on leaf nodes.
- **lifetime-cache-control-extensions**
  Enables you to configure extension tokens to be added to the cache-control header of HTTP response. The WebAccelerator system does not process any of these extensions. It is possible that the origin Web server will send cache-control extensions as well. You can choose whether to preserve them by including the **custom-extension** in the **lifetime-preserve-response-values** list.
- **lifetime-cache-max-age**
  Specifies the amount of time that the WebAccelerator system serves content from the cache before requesting fresh content from the origin Web server. The default value is **4** hours.
- **lifetime-honor-ows**
  Specifies, if enabled, that the WebAccelerator system honors certain cache-control directives from the origin Web server response to determine cache lifetime. The default value is **disabled**.
- **lifetime-honor-ows-values**
  Specifies which Cache-Control directive from the origin Web server response will determine cache lifetime. Available directives are **all-values**, **private**, **no-cache**, **no-store**, **must-revalidate**, **proxy-revalidate**, **max-age**, **s-maxage**, and **expires**. This option is only effective if **lifetime-honor-ows** is enabled.
- **lifetime-honor-request**
  Specifies, if enabled, that the WebAccelerator system honors certain Cache-Control directives from the client's browser request to determine cache lifetime. The default value is **enabled**.

- **lifetime-honor-request-values**
  Specifies which cache-control directive from client's browser request will determine cache lifetime. Available directives are **all-values**, **no-cache**, **no-store**, **max-age**, **max-stale**, and **min-fresh**. This option is only effective if **lifetime-honor-request** is enabled. The default values are **max-age**, **max-stale**, and **min-fresh**.
- **lifetime-http-heuristic**
  Specifies the percentage, based on the HTTP Last-Modified header, that the WebAccelerator system uses to compute TTL values for cached content. For example, if content was modified 30 days ago and the **lifetime-http-heuristic** option is set to 50%, the WebAccelerator system caches the content for 15 days. This option is applicable only if you use the HTTP Last-Modified headers to identify content lifetime. The default value is **50%**. This option is effective only if **lifetime-use-heuristic** is enabled.
- **lifetime-insert-no-cache**
  Specifies, when enabled, that the WebAccelerator system inserts a no-cache directive into the HTTP Cache-Control header, which stops the client's browser from locally caching content. This value overrides the HTTP Cache-Control header cache directives sent to the client by the origin Web server.
- **lifetime-preserve-response**
  Specifies, if enabled, that the WebAccelerator system preserves certain Cache-Control directives from the origin Web server and includes them into client's browser response. The default value is **enabled**.
- **lifetime-preserve-response-values**
  Specifies which Cache-Control directive from the origin web server response will be preserved in response to the client's web browser. Available directives are **all-values**, **private**, **no-cache**, **no-store**, **must-revalidate**, **proxy-revalidate**, **max-age**, **s-maxage**, **expires**, and **custom-extension**. This option is only effective if **lifetime-preserve-response** is enabled. The default value is **all-values**.
- **lifetime-response-max-age**
  Specifies, when enabled, the amount of time that the client's browser should locally store content. This value overrides the max-age and expires the directives in the HTTP Cache-Control header that are sent to the client by the origin web server, only if the new value for the max-age is greater than the value supplied by the origin web server. Modify this value only if there is an acceptable trade off between the freshness of the content served to clients and overall site performance.
- **lifetime-response-s-maxage**
  Specifies, when enabled, the amount of time that the client's browser should locally store shared content. This value overrides the s-maxage and expires the directives in the HTTP Cache-Control header that are sent to the client by the origin web server, only if the new value for the s-maxage is greater than the value supplied by the origin web server. Modify this value only if there is an acceptable trade off between the freshness of the shared content served to clients and overall site performance.

- **lifetime-stand-in-codes**
  Specifies that the WebAccelerator system is allowed to serve stale content from the cache if it is not able to re-validate its freshness with the origin web server. The WebAccelerator system serves invalid content to the downstream proxies or clients if the response code from the origin web server matches one of codes specified with this option. This option is effective only if **cache-stand-in-period** has a non-zero value. The default values are **404**, **500**, and **504**.
- **lifetime-use-heuristic**
  Specifies, when enabled, that the WebAccelerator system uses the percentage from **lifetime-use-heuristic** option to compute TTL values for cached content. The default value is **no**.
- **matching**
  Specifies the collection of matching rules. The rules consist of the HTTP request data type parameters that the WebAccelerator system uses to match an incoming HTTP request to a specified node. The following types of HTTP parameters are available for matching rules: **host**, **path**, **extension**, **query-param**, **unnamed-query-param**, **path-segment**, **cookie**, **user-agent**, **referrer**, **protocol**, **method**, **header**, **client-ip**, and **content-type**.
- **object-min-size**
  Specifies the minimum object size required in order for content matching the associated node to eligible for caching. The default behavior is to use the minimum object size specified by the associated **web-acceleration** profile.
- **object-max-size**
  Specifies the maximum object size allowed for content matching the associated node in order to eligible for caching. The default behavior is to use the maximum object size specified by the associated **web-acceleration** profile.
- **order**
  Specifies the order of the node in the **Policy Tree**. All nodes in the policy must have an order. The order numbers are sequential, staring from 2. Orders 0 and 1 are reserved for internal use. The child node orders must be greater than the order of their parent node. You can change the order of the nodes by updating the order option of the node that you would like to move. The system honors the specified order if it falls within the range of sibling node orders. Otherwise, the system picks the closest valid order number. The remaining nodes are automatically re-ordered to free requested order number. The node order is also used as a last resort to determine which node to use when multiple nodes match the request. The node with a lower order wins. New nodes have their order assigned automatically to make them last among their siblings.
- **proxy**
  Specifies the collection of proxy rules. In general, proxy rules options are relevant to only requests that match their node, rather than to matched responses. The following types of HTTP parameters are available for

proxy rules: **host**, **query-param**, **unnamed-query-param**, **path-segment**, **cookie**, **user-agent**, **referrer**, **protocol**, **method**, **header**, and **client-ip**.

- **proxy-override**
  Specifies the collection of proxy override rules. You can define proxy override rules and associated conditions under which the WebAccelerator system should ignore proxing rules options. The following types of HTTP parameters are available for proxy override rules: **host**, **query-param**, **unnamed-query-param**, **path-segment**, **cookie**, **user-agent**, **referrer**, **protocol**, **method**, **header**, and **client-ip**.
- **request-queueing**
  Specifies, when enabled, that the WebAccelerator system will queue requests for expired or new documents and proxy fewer requests to the origin web server (OWS). If the response is cachable, the response will be served to all waiting requests; if not, the waiting requests will proxy normally.
- **response-codes-cached**
  Specifies the collection of HTTP response codes that determine whether the WebAccelerator system should cache the content. The valid codes are 300, 301, 302, 307, and 410. The codes 200, 201, 203, and 207 are included into the list implicitly. The default values are **300** and **301**.
- **substitutions**
  Specifies the collection of parameter value substitution rules. Some requested pages include hyperlinks that require that specific information appear in the response. You can configure parameter value substitution so that when a query parameter contains identification information for a sites visitors, it prompts the WebAccelerator system to serve different content for the request, based on the specific visitor. Conversely, if parameter value substitution is not configured, the WebAccelerator system uses the value that it cached for the original request, for all subsequent requests after the first, even if the subsequent requests have different values that should be used in the response.
  If you configure parameter value substitution, the WebAccelerator system changes the targeted parameters value on the page served from the cache, so that the parameter you specify appears on the URL embedded in that page.
- **variation**
  Specifies the collection of variation rules. When the WebAccelerator system caches responses from the origin web server, it uses certain HTTP request parameters to create a Unique Content Identifier (UCI). The WebAccelerator system stores the UCI in the form of a compiled response and uses the UCI to easily match future requests to the correct content in its cache. You can configure variation rules to add or modify the parameters on which the WebAccelerator system bases its caching process. If the WebAccelerator system receives two requests that are identical except for the value of a query parameter defined in the variation rule, it creates a different UCI for each, and caches each response under its unique UCI. The following types of HTTP parameters

are available for variation rules: **host**, **query-param**, **unnamed-query-param**, **path-segment**, **cookie**, **user-agent**, **referrer**, **protocol**, **method**, **header**, and **client-ip**.

- **viewstate-cache**
  Specifies, when enabled, that the WebAccelerator system accelerates requests and responses for Web form objects that are generated by ASP.NET web applications. Because the file size of forms can be significant, the WebAccelerator system is able to cache and substitute values, thus reducing the file size and achieving faster performance.
- **viewstate-cache-size**
  Specifies the size of the ViewState object cache in kilobytes. The default value is **100** kilobytes.
- **viewstate-tag**
  Specifies the name of the web form field where the ViewState object is stored. The default value is **__VIEWSTATE**.
- **video-optimization-fast-start**
  Specifies when enabled, that the WebAccelerator system optimizes video by prefetching.
- **video-optimization-max-bitrate**
  Specifies, the maximum bitrate of video that can be allowed in kilobits per sec. The default vaule is 0.
- **video-optimization-insert-ad**
  Specifies, when enabled, that the WebAccelerator system can insert ad into the video.
- **video-optimization-preroll-ad**
  Specifies, when enabled, that the WebAccelerator system can insert ad at the beginning of the video.
- **video-optimization-ad-frequency**
  Specifies the frequency of ad insertion. Units in seconds.
- **video-optimization-ad-policy**
  Specifies the ad policy applicable when processing the video.
- **type**
  Displays the node type. The possible types are:
  - **branch**
    The branch nodes exist only for the purpose of propagating rule parameters to leaf nodes. The WebAccelerator system does not perform matching against branch nodes. Branch nodes can have multiple leaf (child) nodes, as well as child branch nodes.
  - **leaf**
    A leaf node inherits rule parameters from its parent branch node. The WebAccelerator system performs matching only against leaf nodes, and then applies the leaf nodes corresponding acceleration rules to the request.

Http Parameters

Both matching and acceleration rules are identified by the type, and optionally, by the name of HTTP parameters that are used inside the rules. The following types of HTTP parameters are available:

- **content-type**
  A rule that uses the **content-type** parameter is based on type definitions in the **object-type** components. Unlike the HTTP request data types, a matching rule based on content type is specific to the content type parameter that the WebAccelerator system generates for a response. You specify the regular expression that you want a response's content type to match.
- **client-ip**
  A rule that uses the client IP parameter is based on the IP address of the client making the request. The IP address, however, may not always be the address of the client that originated the request. For example, if the client goes through a proxy server, the IP address is the IP address of the proxy server, rather than the client IP address that originated the request. If several clients use a specific proxy server, they all appear to come from the same IP address.
- **cookie:[name]**
  A rule that uses the cookie parameter is based on a particular cookie that you identify by name, and for which you provide a value to match against. This value is usually literal and must appear on the cookie in the request or in a regular expression that matches the request's cookie that appears on the cookie HTTP request headers. These are the same names you use to set the cookies, using the HTTP Set-Cookie response headers. The HTTP request can contain multiple cookies, and the rule identifier must include the name of the cookie separated with colon (:).
- **extension**
  A rule that uses the extension parameter is based on the value that follows the far-right period, in the far-right segment key of the URL path.
- **header:[name]**
  A rule that uses the header parameter is based on a particular header that you identify by name and for which you provide a value to match against. You can use an HTTP request data type header parameter to create rules based on any request header other than one of the recognized HTTP request data types. The HTTP request can contain multiple headers, and the rule identifier must include the name of the header separated with colon (:).
- **host**
  A rule that uses the host parameter is based on the value provided for the HTTP Host request header field. This header field describes the DNS name that the HTTP request is using.
- **method**
  A rule that uses the method parameter is based on whether the request uses the GET or POST method.

- **query-param:[name]**
  A rule that uses the query parameter is based on a particular query parameter that you identify by name and for which you provide a value to match against. The value is usually literal and must appear on the query parameter in the request, or in a regular expression that matches the requests query parameter value. The query parameter can be in a request that uses GET or POST methods. The HTTP request can contain multiple query parameters, and the rule identifier must include the name of the header separated with colon (:).
- **path**
  A rule that uses the path parameter is based on the path portion of the URI. The path is defined as everything in the URL after the host and up to the end of the URL, or up to the question mark (whichever comes first).
- **path-segment:[name]**
  A segment is the portion of a URI path that is delimited by a forward slash (/). For example, in the path: /apps/search/full/complex.jsp, apps, search, full, and complex.jsp all represent path segments. The path can contain multiple segments so the rule identifier must include the name of the segment separated with colon (:). The name can be a segment ordinal or some other string to distinguish it from other segments rules in the same node.
- **protocol**
  A rule that uses the protocol parameter is based on whether the request uses the HTTP or HTTPS protocol.
- **referrer**
  A rule that uses the referrer parameter is based on the value provided for the HTTP Referer in the request header. (Note the misspelling of Referer. This spelling is defined for this request header in all versions of the HTTP specification.) This header provides the URL location that referred the client to the page that the client is requesting. You do not typically base rules on the Referer request header, unless you want your sites behavior to be dependent on the specific referrer. For example, one implementation would be for sites that provide different branding for their pages based on the user's web portal or search engine.
- **unnamed-query-param:[name]**
  An unnamed query parameter is a query parameter that has no equal sign. That is, only the query parameter value is provided in the URL of the request. The HTTP request may contain multiple unnamed query parameters so the rule identifier must include the name of it separated with colon (:). The name can be the ordinal of unnamed query parameter or some other string that can make it distinguishable from other unnamed query parameter rules in the same node.
- **user-agent**
  A rule that uses the user agent parameter is based on the value provided for the HTTP User-Agent in the request header, which identifies the browser that sent the request.

Rule Options

- **active**
  Specifies, when enabled, that the invalidation trigger rule is enabled. You can use this option to disable a specific invalidation trigger rule temporary, without removing it from the policy.
- **arg-all**
  Specifies, when enabled, that the rule matches all HTTP parameters of this type rather than one identified by **arg-name** or **arg-ordinal**. This option is applicable to variation rules **query-param**, **unnamed-query-param**, **path-segment**, **cookie**, and **header**. Such rules serve as a fallback case for defining document variation. All root nodes must include one variation rule of each type with this option enabled. The default value is **disabled**.
- **arg-alias**
- **src-alias**
- **dst-alias**
- **request-data-alias**
  Specifies the user supplied alias for rules that use ordinals to identify HTTP request data. These include the **unnamed-query-param** and **path-segment** rules. The **src-alias** and **dst-alias** options are used in parameter value substitution rules to define aliases for the source and target definitions correspondingly. The **request-data-alias** option defines an alias for the invalidation trigger rules.
- **arg-direction**
- **src-direction**
- **dst-direction**
- **request-data-direction**
  Specifies the direction that the WebAccelerator system uses to count the ordinal of **path-segment**. The **src-direction** and **dst-direction** options are used in parameter value substitution rules to define the ordinal direction for the source and target definitions correspondingly. The **request-data-direction** option defines the ordinal direction for the invalidation trigger rules. The default value is **left-to-right**. The possible values are:
  - **left-to-right**
    The path segment is counted form left to right.
  - **right-to-left**
    The path segment is counted form right to left.
- **arg-name**

- **src-name**
- **dst-name**
- **request-data-name**
  Specifies the name of the parameter type for **query-param**, **cookie**, and **header**. If not specified, **arg-name** option is initialized from the rule name. This option is not effective if **arg-all** is enabled. The **src-name** and **dst-dst** options are used in parameter value substitution rules to define the parameter name for the source and target definitions correspondingly. The **request-data-name** option defines the parameter name for the invalidation trigger rules.
- **arg-ordinal**
- **src-ordinal**
- **dst-ordinal**
- **request-data-ordinal**
  Specifies, in the form of a number, the location of a parameter for **unnamed-query-param** and **path-segment** rules. The numbering starts at 1 and follows the direction specified in the corresponding direction option. This option is not effective if **arg-all** is enabled. The **src-ordinal** and **dst-ordinal** options are used in parameter value substitution rules to define the parameter ordinal for the source and target definitions correspondingly. The **request-data-ordinal** option defines the parameter ordinal for the invalidation trigger rules.
- **broadcast**
  Specifies whether a triggered invalidation rule is broadcast to other members of a multibox deployment. This option is only effective when the application using this policy has **multibox** set to **farm** or **symmetric**.
- **cache-content**
  Specifies the parameter for which the WebAccelerator system must obtain fresh content when the invalidations rule is triggered. The available request types are: **host**, **path**, **extension**, **query-param**, **unnamed-query-param**, **path-segment**, **cookie**, **user-agent**, **referrer**, **protocol**, **method**, **header**, and **client-ip**.

◆ Note

*You must select and configure the **path** parameter for the cached content to invalidate, or the invalidations rule will fail to trigger. All other parameters are optional.*

- **description**
  User-defined description of a rule.
- **dst-type**
  Specifies the HTTP parameter type to use as target definition for the request value substitution rule. A target definition contains a value in the

embedded URL that you want the WebAccelerator system to replace with the value that you specified for the source definition, during assembly. The possible values are:

- **path-segment**
  Specifies that the WebAccelerator system targets the URL parameter, as specified by the **dst-ordinal** and **dst-direction** you define.
- **query-param**
  Specifies that the WebAccelerator system targets the URL parameter, as specified by the **dst-name** you define.
- **unnamed-query-param**
  Specifies that the WebAccelerator system substitutes the URL parameter, as specified by the **dst-ordinal** you define.

◆ **dst-urls**
Specifies the collection of URLs in the request for which you want the WebAccelerator system to replace content.

◆ **request**
Specifies a parameter in the request that triggers the invalidations rule. The available request types are: **host**, **path**, **extension**, **query-param**, **unnamed-query-param**, **path-segment**, **cookie**, **user-agent**, **referrer**, **protocol**, **method**, **header**, and **client-ip**.

◆ Note

*You must select and configure the **path** parameter for the request header criteria, or the invalidations rule will fail to trigger. All other parameters are optional.*

◆ **request-data-type**
Specifies the HTTP request parameter value that the WebAccelerator system should find in its cache and for which it should request updated content from the origin Web server. The default value is **undefined**. The following types of HTTP parameters are available:

- **host**
- **query-param**
- **unnamed-query-param**
- **path-segment**
- **cookie**
- **user-agent**
- **referrer**

- **header**

- **client-ip**
  Specifies that the WebAccelerator system should use the corresponding value from the request that triggered the invalidation. Additional data, if required to identify the value, must be specified in the **request-data-name**, **request-data-ordinal**, and **request-data-direction** options. The **values** option is ignored.
- **undefined**
  Specifies that the WebAccelerator system should not use any values from the request that triggered the invalidation. You must add a value into the **values** option with which to compare the cached content.

◆ **src-type**
Specifies the HTTP parameter type to use as source definition for the request value substitution rule. A source definition contains the value that the WebAccelerator system embeds in the URL, in place of the cached (target definition) value, during substitution. Typically, the source definition is a specific request element, such as a particular query parameter; however, you can specify another source type, such as a random number. The possible values are:

- **path-segment**
  Specifies that the WebAccelerator system substitutes the URL parameter, as specified by the **src-ordinal** and **src-direction** options you define.
- **query-param**
  Specifies that the WebAccelerator system substitutes the URL parameter, as specified by the **src-name** option you define.
- **randomizer**
  Specifies that the WebAccelerator system generates a random number and places that number on the targeted location in an embedded URL.
- **request-url**
  Specifies that the WebAccelerator system is limited to target-specific URLs embedded in a page, as defined in the prefix that an embedded URL must match before the WebAccelerator system performs substitution. If you use the request URL as the source, the WebAccelerator system uses the entire request URL as the value to substitute.
- **unnamed-query-param**
  Specifies that the WebAccelerator system substitutes the URL parameter, as specified by the **src-ordinal** option you define.

◆ **src-url**
Specifies whether the request URL is a **relative** URL or an **absolute** URL. The default value is **absolute**.

◆ **value-case-sensitive**
Specifies, when enabled, that the HTTP parameter must be matched against supplied value(s) in case sensitive manner. The default value is **no**.

- **values**
  Values are a collection of rule parameters that enable you to specify different parameter values for the same rule. Most rules allow only one value, while variation rules support multiple values. Each value can prompt a different behavior by the WebAccelerator system. All variation rules must include at least one value with **match-all** option enabled. A value can be represented by actual string, regex, or multiple strings, or regexes separated by space ( ).

Rule Value Options

- **can-be-empty**
  Specifies, when enabled, that the defined HTTP request parameter is included in the request, but has no value (is an empty string). The default value is **no**.
- **can-be-missing**
  Specifies, when enabled, that the defined HTTP request parameter is absent from the request. The default value is **no**.
- **invert-match**
  Specifies, when enabled, that the defined HTTP request parameter does not match the associated regular expression that you defined. The default value is **no**.
- **match-all**
  Specifies, when enabled, that the defined HTTP request parameter matches all possible values. This option is available only for variation rule values as a fallback case. Each variation rule must have at least one value with this option enabled. The default value is **no**.
- **cache-as**
  Specifies whether the associated value should prompt the WebAccelerator system to reply to matched requests with the **same** or **different** content. This option is available only for variation rule values.

See Also

create, *delete*, *edit*, *list*, *modify*, *show*, *tmsh*

roi-statistics

Provides ROI statistics for WAM application.

Syntax

Provides ROI statistics for configured **application** within the **wam** module.

Display

```
show roi-statistics
show roi-statistics [application-name]
  (default | exa | gig | kil | meg | peta | raw | tera | yotta | zetta)
  field-fmt
```

Description

You can use the **roi-statistics** component to view the ROI statistics of configured WAM application.

Examples

show roi-statistics my_application

The show command will display ROI statistics for the configured WAM application.

See Also

show, *tmsh*

113

wam resource

- Introducing the wam resource module
- Alphabetical list of components

Introducing the wam resource module

You can use the tmsh components that reside within the wam module to configure URL resources for BIG-IP® WebAccelerator™. For more information about the tmsh hierarchical structure, see Chapter 2, *Understanding and Using the Traffic Management Shell*.

Alphabetical list of components

The remainder of this chapter lists the tmsh components that are available in the wam resource module.

concat-set

Configures concatenation sets for WebAccelerator for use in JavaScript/CSS concatenation

Syntax

Configure the **concat-set** within the **wam resource** module using the syntax shown in the following sections.

Create/Modify

```
create concat-set [name]
modify concat-set [name]
   app-service [[string] | none]
   url [url]
   type [css|js]
   members [string ] ...
```

Display

```
list concat-set [name ...]
```

Delete

```
delete concat-set [name ...]
```

Description

You can use the **concat-set** component to manage the concatenation sets used by the WebAccelerator JavaScript and CSS concatenation feature. A concatenation set must be created, then enabled and activated in the configuration on a WebAccelerator policy node.

Examples

create concat-set testSet url http://www.example.com/concatSet.css type css

Creates a set whose URL will be **http://www.example.com/concatSet.css** for use
in concatenation.

list concat-set testSet

Displays properties of the concatenation set named **testSet**.

delete concat-set testSet

Deletes concatenation set named **testSet**.

Options

- **app-service**
  Specifies the name of the application service to which the object belongs. The default value is **none**. **Note:** If the **strict-updates** option is **enabled** on the application service that owns the object, you cannot modify or delete the object. Only the application service can modify or delete the object.
- **url**
  Specifies the URL that will be used to generate the concatenated link.
- **type**
  Either "css" or "js". Specifies whether the set is to be used for CSS or JavaScript concatenation.
- **members**
  Specifies the members of this set. The set members are the URL resources that are defined by the **wam resource url**.

See Also

create, *delete*, *edit*, *list*, *modify*, *tmsh*

domain-list

Configures a list of domains for WebAccelerator for use in inserting DNS prefetch tags.

Syntax

Configure the **domain-list** component within the **wam resource** module using the syntax shown in the following sections.

Create/Modify

```
create domain-list [name]
modify domain-list [name]
   app-service [[string] | none]
   description [[string] | none]
   domains
       [add | delete | none| replace-all-with] {
           [string] ...
   }
```

Display

```
list domain-list [name ...]
```

Delete

```
delete domain-list [name ...]
```

Description

You can use the **domain-list** component to manage the domain list resources used by the WebAccelerator DNS prefetching feature. A domain-list must be created, then added to the appropriate domain-lists on a WebAccelerator policy node in order for the domains within the domain list to be inserted into a document.

Examples

create domain-list my_domain_list domains add {example.com example2.com}

Creates a domain list resource for the domains **example.com** and **example2.com** for use
in inserting DNS prefetch tags.

list domain-list my_domain_list

Displays properties of the domain-list resource named **my_domain_list**.

delete domain-list my_domain_list

Deletes the domain-list resource named **my_domain_list**.

Options

- **app-service**
  Specifies the name of the application service to which the object belongs. The default value is **none**. **Note:** If the **strict-updates** option is **enabled** on the application service that owns the object, you cannot modify or delete the object. Only the application service can modify or delete the object.
- **description**
  User defined description.
- **domains**
  Specifies the domains described by the domain list resource.

See Also

create, *delete*, *edit*, *list*, *modify*, *show*, *tmsh*

url

Configures a URL resource for WebAccelerator for use in reordering whitelists

Syntax

Configure the **url** component within the **wam resource** module using the syntax shown in the following sections.

Create/Modify

```
create url [name]
modify url [name]
   app-service [[string] | none]
   url [url]
   type [css|js]
```

Display

```
list url [name ...]
```

Delete

```
delete url [name ...]
```

Description

You can use the **url** component to manage the URL resources used by the WebAccelerator JavaScript and CSS reordering features. A URL resource must be created, then added to the appropriate whitelist on a WebAccelerator policy node in order for the corresponding URL to be reordered.

Examples

create url test.css url http://www.example.com/test.css type css

Creates a URL resource for the URL **http://www.example.com/test.css** for use
in CSS reordering whitelists.

list url test.css

Displays properties of the URL resource named **test.css**.

delete url test.css

Deletes the URL resource named **test.css**.

Options

- **app-service**
  Specifies the name of the application service to which the object belongs. The default value is **none**. **Note:** If the **strict-updates** option is **enabled** on the application service that owns the object, you cannot modify or delete the object. Only the application service can modify or delete the object.
- **url**
  Specifies the URL described by the URL resource.
- **type**
  Either "css" or "js". Specifies whether the URL resource is to be used for CSS or JavaScript reordering.

See Also

create, *delete*, *edit*, *list*, *modify*, *show*, *tmsh*

114

wom

- Introducing the wom module
- Alphabetical list of components

Introducing the wom module

You can use the tmsh components that reside within the wom module to configure WAN optimization. For more information about the tmsh hierarchical structure, see Chapter 2, *Understanding and Using the Traffic Management Shell*.

Alphabetical list of components

The remainder of this chapter lists the tmsh components that are available in the wom module.

advertised-route

Configures a route advertised by the local endpoint to remote endpoints for WAN optimization.

Syntax

Configure the **advertised-route** component within the **wom** module using the syntax in the following sections.

Create/Modify

```
create advertised-route [name]
modify advertised-route [name | all]
    app-service [[string] | none]
    description [string]
    dest [ip address/netmask]
    include [disabled | enabled]
    label [value]
    metric [integer]
    origin [configured | discovered | manually-saved | persistable]
```

Display

```
list advertised-route
show advertised-route
    all
    all-properties
    app-service
    running-config
    non-default properties
    one-line
```

Delete

```
delete advertised-route [name]
```

Description

You can use the **advertised-route** component to configure a subnet that the system can reach through the local endpoint. You can specify a netmask or use slash format.

Routes are advertised to all connected WAN Optimization Managers. The remote endpoints use the subnet configuration information to determine peer routing and optimization actions.

Examples

list advertised-route all

Displays all endpoint advertised routes for the local WAN Optimization Manager.

delete advertised-route adv_rt2

Deletes the advertised route **adv_rt2**.

Options

- **app-service**
  Specifies the name of the application service to which the object belongs. The default value is **none**. **Note:** If the **strict-updates** option is **enabled** on the application service that owns the object, you cannot modify or delete the object. Only the application service can modify or delete the object.
- **description**
  User defined description.
- **dest**
  Specifies the IP address and netmask of the advertised route.
- **include**
  Enables or disables the inclusion of this route in the optimization of traffic. This option allows you to define a subset of IP addresses to exclude from optimization within a larger included subnet. An excluded endpoint advertised route must be a valid address range subset of an included endpoint advertised route. The default is **enabled**.
- **label**
  Specifies an optional descriptive label for this route.
- **metric**
  Specifies a routing number to select between WAN Optimization Manager pairs. The higher the number, the more expensive the route in terms of resources. Not currently implemented.
- **origin**
  Specifies whether the route was discovered automatically or configured manually. You can change the origin from **discovered** to **persistable**, if you want to save the route to the file **bigip_local.conf** when you use the command **save config**. After you run the command **save config**, this attribute changes to **manually saved**. Endpoints that have the attribute **discovered** are not saved to the file **bigip_local.conf**.
  The options are:
  - **configured**
    Indicates that you manually configured this route. The system automatically sets this value, and you cannot change it.
  - **discovered**
    Indicates that the system automatically discovered this route. Note that route for which the value of the **origin** property is **discovered** are not saved to the file **bigip_local.conf**.

- **manually-saved**
  After you run the command **save / sys config**, the value of the **origin** property that was set to **persistable** changes to **manually-saved**. Note that after the system changes the value to **manually-saved**, you cannot change it again.
- **persistable**
  Change the origin from **discovered** to **persistable**, if you want to save the route to the file **bigip_local.conf** when you use the command **save / sys config**.

See Also

create, *delete*, *list*, *local-endpoint*, *modify*, *remote-endpoint*, *server-discovery*, *show*, *tmsh*

deduplication

Configures symmetric data deduplication for WAN optimization.

Syntax

Configure the **deduplication** component within the **wom** module using the syntax in the following sections.

Modify

```
modify deduplication
    codec [sdd-v2 | sdd-v3]
    [disabled | enabled]
    max-endpoint-count [integer]
```

Display

```
list deduplication
show running-config deduplication
    dictionary-size
    one-line
```

Description

You can use the **deduplication** component to configure symmetric data deduplication, which compresses data over the WAN by identifying and removing repetitive data patterns.

Examples

list deduplication

Displays all the deduplication settings.

modify deduplication max-endpoint-count 4

Sets the maximum number of remote endpoints to **4**.

Options

- **codec**
  Specifies which algorithm the system uses for deduplication.
  The options are:
  - **sdd-v2**
    Used for low number of spokes, such as for data center to data center replication.

  - **sdd-v3**
    Used for high number of spokes, such as for connecting multiple remote sites or mesh topologies.

- **dictionary-size**
  Displays the current size of the dictionary, which deduplication uses to look up byte patterns.
- **[disabled | enabled]**
  Enables or disables deduplication. The default value is **enabled**. Note that if you enable or disable deduplication, you must then restart the BIG-IP WOM system using **bigstart restart**, or the change takes effect the next time the BIG-IP device reboots.
- **max-endpoint-count**
  Specifies the maximum number of concurrent remote endpoints supported by symmetric data deduplication. For codec **sdd-v3**, the system sets the value at **128**.

See Also

datastor, *list*, *modify*, *show*, *tmsh*, *isession*,

diagnose-conn

Diagnoses network connection problems.

Syntax

run diagnose-conn

Description

You can use the **diagnose-conn** component within the **wom** module to display diagnostic information about network connections.

See Also

run, *tmsh*, *verify-config*

endpoint-discovery

Configures automatic discovery of remote endpoints for WAN optimization.

Syntax

Configure the **endpoint-discovery** component with the **wom** module using the syntax in the following sections.

Modify

```
modify endpoint-discovery
    auto-save [disabled | enabled]
    description [string]
    discoverable [disabled | enabled]
    discovered-endpoint [disabled | enabled]
    icmp-max-requests [integer]
    icmp-min-backoff [integer]
    icmp-num-retries [integer]
    max-endpoint-count [integer]
    mode [disable | enable-all | enable-icmp | enable-tcp]
reset-stats endpoint-discovery
```

Display

```
list endpoint-discovery
show running-config endpoint-discovery
    all-properties
    non-default-properties
    one-line
show endpoint-discovery
    (default | exa | gig | kil | meg | peta | raw | tera | yotta | zetta)
```

Description

You can use the **endpoint-discovery** component to specify parameters for automatically discovering remote endpoints for WAN optimization. These endpoints are configured WAN Optimization Managers on remote BIG-IP® systems that advertise themselves to the configured WAN Optimization Manager on the local BIG-IP system.

Examples

modify endpoint-discovery max-endpoint-count 10

Limits the number of remote endpoints that can be discovered to ten. After discovering ten remote endpoints, the WOM stops sending probe messages.

list endpoint-discovery all-properties

Displays the configuration parameters for the discovery of remote endpoints.

Options

- **auto-save**
  Specifies whether the system automatically saves remote endpoints that it discovers. The default value is **enabled**.
- **description**
  User defined description.
- **discoverable**
  Specifies whether the WAN Optimization Manager responds to probe messages it receives from WAN Optimization Managers on remote BIG-IP systems. The default value is **enabled**.
- **discovered-endpoint**
  Specifies whether the WAN Optimization Manager sends out probe messages to discover other WAN Optimization Managers on remote BIG-IP systems in the network. The default value is **enabled**.
- **icmp-max-requests**
  Specifies the maximum number of ICMP probe message requests, after which the system stops sending probe message requests until at least one message is cleared from the queue by either a timeout or a response. The default value is **1024**.
- **icmp-min-backoff**
  Specifies the maximum number of seconds to wait before abandoning an ICMP probe message request and resending it. The range is from **0** to **255**. The default value is **5**.
- **icmp-num-retries**
  Specifies the maximum number of times the system sends an ICMP probe message request for a single flow. The range is from **0** to **255**. The default value is **10**.
- **max-endpoint-count**
  Specifies the highest number of endpoints for the system to discover before it stops sending probe messages. The range is from **0** to **255**. The default value is **0**, which indicates no limit.
- **mode**
  Specifies the type of probe messages the system should send. The default value is **enable-all**.
  The options are:
  - **disable**
    Turns off probe messages.
  - **enable-icmp**
    Sends only ICMP probe messages.
  - **enable-tcp**
    Sends only TCP probe messages.

- **enable-all**
  Sends both ICMP and TCP probe messages.

See Also

list, *modify*, *show*, *tmsh*, *local-endpoint*, *remote-endpoint*, *server-discovery*

local-endpoint

Configures the local endpoint for the WAN Optimization Manager.

Syntax

Configure the **local-endpoint** component within the **wom** module using the following syntax.

Create/Modify

```
create local-endpoint
modify local-endpoint
    addresses [add | delete | replace-all-with] {
      [ip address]
    }
    addresses none
    allow-nat [disabled | enabled]
    description [string]
    endpoint [disabled | enabled]
    internal-forwarding [disabled | enabled]
    ip-encap-mtu [unsigned integer]
    ip-encap-profile [none | profile name]
    ip-encap-type [gre | ipip | ipsec | none]
    no-route [drop | passthru]
    server-ssl [none | profile name]
    snat [local | none | remote]
    tunnel-port [unsigned integer]
```

Display

```
list local-endpoint
show local-endpoint
show running-config local-endpoint
    all-properties
    non-default-properties
    one-line
```

Delete

```
delete local-endpoint
```

Description

You can use the **local-endpoint** component to modify the settings for the local endpoint for the WAN Optimization Manager on the local BIG-IP® system.

Examples

modify local-endpoint allow-nat disabled

Disables the **allow-nat** option, specifying that the system does not accept connections for traffic behind a Network Address Translation (NAT) device.

list local-endpoint all-properties

Displays all of the properties of the **local-endpoint** component.

Options

- **addresses**
  Specifies a single IP address the system uses for the local endpoint. The IP address must be in the same subnet as a self IP address on the BIG-IP® system.
- **allow-nat**
  When enabled, specifies that the system accepts connections for traffic behind a Network Address Translation device. The default value is **enabled**.
- **description**
  User defined description.
- **endpoint**
  When **enabled**, specifies that the local endpoint is available for initiating and receiving optimized traffic. The default value is **enabled**.
  To turn off WAN optimization on this endpoint, use **disabled**.
- **internal-forwarding**
  When **enabled**, specifies that the local endpoint is available for forwarding internal traffic to remote endpoints. The default value is **disabled**.
  This parameter works only if **internal-forwarding** for remote-endpoint is set to **default**.
- **ip-encap-mtu**
  Specifies the maximum transfer unit for IP encapsulated traffic.
- **ip-encap-profile**
  Specifies the name of the profile with the encapsulation settings. This profile must be of the type specified for the setting **ip-encap-type**.
- **ip-encap-type**
  Specifies the type of IP layer encapsulation to perform on iSession™ traffic.
  The default value is **none**. The options are:
  - **gre**
    The system uses the Generic Routing Encapsulation (GRE) tunneling protocol.
  - **ipip**
    The system uses the IP over IP (IPIP) tunneling protocol.
  - **ipsec**
    The system uses IP security (IPsec) encapsulation.
  - **none**
    No IP encapsulation takes place.

- **no-route**
  Specifies what the system does with traffic for which there is no remote endpoint to complete the iSession connection.
  The default value is **passthru**. The options are:
  - **drop**
    The system terminates the traffic flow.
  - **passthru**
    The traffic flow continues without an iSession connection.
- **server-ssl**
  Specifies the default server SSL profile the system uses for all encrypted outbound connections. The default value is **none**.
- **snat**
  Specifies the IP address the system uses for incoming traffic as the source IP address of the TCP connection between the WAN Optimization Manager and the server.
  The default value is **none**. The options are:
  - **local**
    The system uses the endpoint IP address closest to the destination. Use this setting to make sure the return route also goes through the BIG-IP system, so that both sides of the connection can be optimized. This setting is useful if responses returning from the server to the client would not normally pass through the BIG-IP system.
  - **none**
    The system uses the original connecting client IP address.
  - **remote**
    The system uses the source IP address of the incoming iSession connection. Use this setting when an appliance that uses NAT is located between the WAN Optimization endpoints.
- **tunnel-port**
  Specifies the number of the port on the local endpoint that the WAN Optimization Manager uses for control connections. The port must have access through the firewall. The range is from **1** to **65535**. The default value is **443**.

See Also

list, *modify*, *show*, *tmsh*, *advertised-route*, *remote-endpoint*

remote-endpoint

Configures one or more remote endpoints for the WAN Optimization Manager.

Syntax

Configure the **remote-endpoint** component within the **wom** module using the following syntax.

Create/Modify

```
create remote-endpoint [name]
modify remote-endpoint [name]
    address [ip address]
    allow-routing [disabled | enabled]
    app-service [[string] | none]
    dedup-action [none | cache-refresh]
    description [string]
    endpoint [disabled | enabled]
    internal-forwarding [default | disabled | enabled]
    ip-encap-mtu [unsigned integer]
    ip-encap-profile [none | profile name]
    ip-encap-type [default | gre | ipip | ipsec | none]
    origin [configured | discovered | manually-saved | persistable]
    server-ssl [none | profile name]
    snat [default | local | none | remote]
    tunnel-encrypt [disabled | enabled]
    tunnel-port [unsigned integer]
reset-stats remote-endpoint
```

Display

```
list remote-endpoint
list remote-endpoint [name]
show running-config remote-endpoint
show running-config remote-endpoint [name]
    all-properties
    dedup-codec
    non-default-properties
    one-line
show remote-endpoint
show remote-endpoint [name]
    (default | exa | gig | kil | meg | peta | raw | tera | yotta | zetta)
```

Delete

```
delete remote-endpoint [name]
```

◆ Note

*If you delete a remote endpoint without also disabling the **endpoint-discovery** component, the remote endpoint may reappear as it is rediscovered. To remove a remote endpoint from traffic initiated by this WAN Optimization Manager, set the **endpoint** option of the **remote-endpoint** component to **disabled**.*

Description

You can use the **remote-endpoint** component to create, modify, or delete a remote endpoint for traffic from the local WAN Optimization Manager.

Examples

modify remote-endpoint 13.16.0.5 endpoint disabled

Disables the WAN optimization connection to the remote endpoint that is named **13.16.0.5**.

list remote-endpoint all-properties

Displays all the properties of all the remote endpoints for traffic from the local WAN Optimization Manager.

Options

- **allow-routing**
  Specifies whether there is a route from the local endpoint to this remote endpoint through which the local endpoint can establish connections. The default value is **enabled**.
- **address**
  Specifies the IP address of the remote endpoint.
- **app-service**
  Specifies the name of the application service to which the object belongs. The default value is **none**. **Note:** If the **strict-updates** option is **enabled** on the application service that owns the object, you cannot modify or delete the object. Only the application service can modify or delete the object.
- **description**
  User defined description.
- **dedup-action**
  Clears the cache used for symmetric data deduplication on the specified remote endpoint and immediately resets the value to **none**.

- **dedup-codec**
  Displays the deduplication codec used by the remote endpoint: **sdd-v2** or **sdd-v3**.
- **endpoint**
  When **enabled**, specifies that traffic can be optimized between the local and remote endpoints. The default value is **enabled**.

◆ Note

Disabling a remote endpoint affects only the connection between the local endpoint and this remote endpoint.

- **internal-forwarding**
  When **enabled**, specifies that the remote endpoint is available for forwarding internal traffic.
  When **disabled**, specifies that the remote endpoint is NOT available for forwarding internal traffic.
  When **default**, specifies that forwarding internal traffic is managed by the **local-endpoint.internal-forwarding** setting.
  The default value is **default**.
- **ip-encap-mtu**
  Specifies the maximum transfer unit for IP encapsulated traffic. The default value is **0**.
- **ip-encap-profile**
  Specifies the name of a profile with encapsulation settings. This profile must be of the type specified for the setting **ip-encap-type**.
- **ip-encap-type**
  Specifies the type of IP layer encapsulation performed on iSession traffic.
  The default value is **default**. The options are:
  - **default**
    The system uses the **ip-encap-type** value set for the local endpoint.
  - **gre**
    The system uses the Generic Routing Encapsulation (GRE) tunneling protocol.
  - **ipip**
    The system uses the IP over IP (IPIP) tunneling protocol.
  - **ipsec**
    The system uses IP security (IPsec) encapsulation.
  - **none**
    No IP encapsulation takes place.
- **origin**
  Specifies whether the remote endpoint was discovered automatically or configured manually.
  The options are:
  - **configured**
    Indicates that you manually configured this remote endpoint. The system automatically sets this value, and you cannot change it.

- **discovered**
  Indicates that the system automatically discovered this remote endpoint. Note that endpoints for which the value of the **origin** property is **discovered** are not saved to the file **bigip_local.conf**.
- **manually-saved**
  After you run the command **save / sys config**, the value of the **origin** property that was set to **persistable** changes to **manually-saved**. Note that after the system changes the value to **manually-saved**, you cannot change it again.
- **persistable**
  Change the origin from **discovered** to **persistable**, if you want to save the endpoint to the file **bigip_local.conf** when you use the command **save / sys config**.

◆ **server-ssl**
Specifies the server SSL profile the system uses to connect to this remote endpoint. This setting overrides the **server-ssl** setting for the **local-endpoint** component. The default value is **none**.

◆ **snat**
Specifies the IP address the system uses as the source IP address of the TCP connection between the WAN Optimization Manager and the server.
The default value is **default**. The options are:

- **default**
  The system uses the **snat** value set for the **local-endpoint** component.
- **local**
  The system uses the endpoint IP address closest to the destination. Use this setting to make sure the return route also goes through the BIG-IP system, so that both sides of the connection can be optimized. This setting is useful if responses returning from the server to the client would not normally pass through the BIG-IP system.
- **none**
  The system uses the original connecting client IP address.
- **remote**
  The system uses the source IP address of the incoming iSession connection. Use this setting when an appliance that uses NAT is located between the WAN Optimization Manager endpoints.

◆ **tunnel-encrypt**
Enables or disables encryption of traffic passing between the two WAN Optimization Managers. The default value is **enabled**

◆ **tunnel-port**
Specifies whether to use a specific port for traffic optimized to this endpoint or to use port transparency (**0**). The default value is **443**.

See Also

create, *delete*, *list*, *modify*, *show*, *tmsh*, *advertised-route*, *local-endpoint*

remote-route

Displays the destination routes learned from the remote endpoints.

Syntax

Display the **remote-route** component within the **wom** module using the syntax in the following section.

Display

```
show remote-route
    (default | exa | gig | kil | meg | peta | raw | tera | yotta | zetta)
    detail
```

Description

You can use the **remote-route** component to view the subnets that the system can reach through the remote endpoint(s). The system can optimize traffic destined for these subnets.

Examples

show remote-route

Displays the subnets reachable through the remote endpoint(s) configured on the WAN Optimization Manager.

show remote-route detail

Displays detailed information about the remote endpoint(s) through which the displayed subnets can be reached.

See Also

show, *tmsh*, *advertised-route*, *remote-endpoint*, *server-discovery*,

server-discovery

Configures the dynamic discovery of servers that can be reached through the local endpoint and the routes to reach them.

Syntax

Configure the **server-discovery** component within the **wom** module using the syntax in the following sections.

Modify

```
modify server-discovery
    auto-save [disabled | enabled]
    description [string]
    filter-mode [exclude | include]
    idle-time-limit [integer]
    ip-ttl-limit [integer]
    max-server-count [integer]
    min-idle-time [integer]
    min-prefix-length-ipv4 [integer]
    min-prefix-length-ipv6 [integer]
    mode [disabled | enabled]
    rtt-threshold [integer]
    subnet-filter [add | delete | none | replace-all-with] {
      [ip address]
     }
    time-unit [days | hours | minutes]
```

Display

```
list server-discovery
show running-config server-discovery
    all-properties
    auto-save
    current-module
    description
    filter-mode
    idle-time-limit
    ip-ttl-limit
    max-server-count
    min-idle-time
    min-prefix-length-ipv4
    min-prefix-length-ipv6
    mode
    non-default-properties
    one-line
    rtt-threshold
    subnet-filter
    time-unit
```

Description

You can use the **server-discovery** component to configure the dynamic discovery of servers and the routes to reach them through the local endpoint. The local endpoint advertises these routes to any remote endpoints to which it is connected.

Examples

list server-discovery all-properties

Displays the settings for dynamic discovery of advertised routes.

modify server-discovery mode disabled

Disables the dynamic discovery of advertised routes.

Options

- **auto-save**
  Specifies whether the system automatically saves the subnets that it discovers that can reached through the local endpoint. The default value is **enabled**.
- **description**
  User defined description.
- **filter-mode**
  Specifies whether the subnets you add using the attribute **subnet-filter** are excluded from or included in the discovery of advertised routes. If you specify **include**, and do not specify any IP addresses, no subnets are discovered. The default is **exclude** with no IP addresses specified, which means that all advertised routes that conform to the specified attributes are discovered.
- **idle-time-limit**
  Specifies the maximum length of time a route can be idle without being removed from discovery. The default value is **0**. Use the attribute **time-unit** to set the unit of measure. Use the attribute **min-idle-time** to set the minimum length of idle time.
- **ip-ttl-limit**
  Specifies the number of network segments on which a packet is allowed to travel before the route is removed from discovery. The more routers a packet travels through, the smaller the ip ttl value is. The range is **0** to **255**. The default value is **5**.
- **max-server-count**
  Specifies the highest number of servers the system discovers before it stops looking. The default value is **50**.
- **min-idle-time**
  Specifies the minimum length of time a route must be idle before being removed from discovery. The default value is **0**, which indicates that idle

time is not considered in discovery. Use the attribute **time-unit** to set the unit of measure. Use the attribute **idle-time-limit** to set the maximum length of idle time.

- **min-prefix-length-ipv4**
  Specifies the minimum prefix length for route aggregation in IPV4 networks. The range is **0** to **32**. The default value is **32**.
- **min-prefix-length-ipv6**
  Specifies the minimum prefix length for route aggregation in IPV6 networks. The range is **0** to **128**. The default value is **128**.
- **mode**
  Enables or disables the dynamic discovery of servers that can be reached through the local endpoint. For server discovery to take place, the setting **mode** of the component **wom endpoint-discovery** must not be set to **disabled**.
- **rtt-threshold**
  Specifies that the system does not add servers it discovers with a round-trip time greater than this value, in milliseconds. The default value is **10**.
- **subnet-filter**
  Specifies the IP addresses of the subnets to include in or exclude from the discovery of advertised routes, depending on the setting you selected for the attribute **filter-mode**. The default is **none**. If you selected **include** for the attribute **filter-mode**, and do not specify any IP addresses, no subnets are discovered.
- **time-unit**
  Specifies the unit of measure (**days**, **hours**, or **minutes**) for the length of idle time specified using the attributes **idle-time-limit** and **min-idle-time**.

See Also

list, *modify*, *show*, *tmsh*, *advertised-route*, *endpoint-discovery*, *local-endpoint*, *remote-route*

verify-config

Checks the WAN Optimization Manager configuration.

Syntax

run verify-config

Description

You can use the **verify-config** component within the **wom** module to display configuration information about the WAN Optimization Manager that can be used for troubleshooting.

See Also

run, *tmsh*, *diagnose-conn*

115

wom profile

- Introducing the wom profile module
- Alphabetical list of components

Introducing the wom profile module

You can use the tmsh components that reside within the wom profile module to configure profiles for WAN optimization. For more information about the tmsh hierarchical structure, see Chapter 2, *Understanding and Using the Traffic Management Shell*.

Alphabetical list of components

The remainder of this chapter lists the tmsh components that are available in the wom profile module.

cifs

Configures a Common Internet File System (CIFS) profile.

Syntax

Configure the **cifs** component within the **wom profile** module using the syntax shown in the following sections.

Create/Modify

```
create cifs [name]
modify cifs [name]
    app-service [[string] | none]
    defaults-from [ [name] | none]
    description [string]
    fast-close [disabled | enabled]
    fast-set-file-info [disabled | enabled]
    office-2003-extended [disabled | enabled]
    read-ahead [disabled | enabled]
    record-replay [disabled | enabled]
    write-behind [disabled | enabled]
```

Display

```
list cifs
list cifs [ [ [name] | [glob] | [regex] ] ... ]
show running-config cifs
show running-config cifs [ [ [name] | [glob] | [regex] ] ... ]
    all-properties
    app-service
    non-default-properties
    one-line
    partition
show cifs
show cifs [ [ [name] | [glob] | [regex] ] ... ]
    (default | exa | gig | kil | meg | peta | raw | tera | yotta | zetta)
```

Delete

```
delete cifs [name]
```

Description

You can use the **cifs** component to manage a CIFS profile.

Examples

create cifs my_cifs_profile

Creates a CIFS profile named **my_cifs_profile** using the system defaults.

modify cifs my_cifs_profile fast-close disabled

Turns off **fast-close** for the CIFS profile named **my_cifs_profile**.

Options

- **app-service**
  Specifies the name of the application service to which the object belongs. The default value is **none**. **Note:** If the **strict-updates** option is **enabled** on the application service that owns the object, you cannot modify or delete the object. Only the application service can modify or delete the object.
- **defaults-from**
  Specifies the profile that you want to use as the parent profile. The new profile inherits all settings and values from the parent profile specified. The default value is **cifs**.
- **description**
  User defined description.
- **fast-close**
  Specifies whether the system speeds up file close operations by fulfilling them through the WAN Optimization Manager closer to the request initiator. The default value is **enabled**.
- **fast-set-file-info**
  Specifies whether the system speeds up file metadata change requests by fulfilling the requests through the WAN Optimization Manager closer to the request initiator. The default value is **enabled**.
- **glob**
  Displays the items that match the **glob** expression. See **help glob** for a description of **glob** expression syntax.
- **name**
  Specifies a unique name for the component. This option is required for the commands **create**, **delete**, and **modify**.
- **office-2003-extended**
  Specifies whether the system performs read-ahead operations based on parsing the Microsoft CDF file and understanding its structure. The default value is **enabled**.
- **partition**
  Displays the administrative partition within which the component resides.
- **read-ahead**
  Specifies whether the system speeds up CIFS file downloads by prefetching the file data on the WAN Optimization Manager closer to the request initiator. The default value is **enabled**.
- **record-replay**
  Specifies whether the system opens CIFS files faster by performing more intelligent read-ahead operations. The default value is **enabled**.

- **regex**
  Displays the items that match the regular expression. The regular expression must be preceded by an at sign (@[regular expression]) to indicate that the identifier is a regular expression. See **help regex** for a description of regular expression syntax.
- **write-behind**
  Specifies whether the system speeds up CIFS file uploads to the server by fulfilling write requests through the WAN Optimization Manager closer to the request initiator. The default value is **enabled**.

See Also

create, *delete*, glob, *list*, *virtual*, *modify*, regex, *show*, *tmsh*

isession

Configures an iSession profile.

Syntax

Configure the **iSession** component within the **wom profile** module using the following syntax.

Create/Modify

```
create isession [name]
modify isession [name]
    adaptive-compression [disabled | enabled]
    app-service [[string] | none]
    compression [disabled | enabled]
    compression-codecs [add | delete | none | replace-all-with] {
        bzip2
        deflate
        lzo
    }
    data-encryption [disabled | enabled]
    deduplication [disabled | enabled]
    defaults-from [ [name] | none]
    deflate-compression-level [integer]
    description [string]
    mode [disabled | enabled]
    port-transparency [disabled | enabled]
    reuse-connection [disabled | enabled]
    target-virtual [none | host-match-all | host-match-no-isession |
virtual-match-all]
reset-stats isession
reset-stats isession [ [ [name] | [blog] | [regex] ] ... ]
```

Display

```
list isession
list isession [ [ [name] | [glob] | [regex] ] ... ]
show running-config isession
show running-config isession [ [ [name] | [glob] | [regex] ] ... ]
    all-properties
    app-service
    non-default-properties
    one-line
    partition
show isession
show isession [ [ [name] | [glob] | [regex] ] ... ]
    (default | exa | gig | kil | meg | peta | raw | tera | yotta | zetta)
    field-fmt
    global
```

Delete

```
delete isession [name]
```

Description

You can use the **isession** component to manage an iSession profile.

Examples

create isession my_isession_profile defaults-from isession

Creates an iSession profile named **my_isession_profile** using the system defaults.

modify isession my_isession_profile deduplication disabled

Turns off **deduplication** for the iSession profile named **my_isession_profile**.

Options

- **adaptive-compression**
  Enables or disables the automatic selection of the optimal compression algorithm for the current traffic, based on link speed. The system can use only compression algorithms that are specified. The default value is **enabled**.
- **app-service**
  Specifies the name of the application service to which the object belongs. The default value is **none**. **Note:** If the **strict-updates** option is **enabled** on the application service that owns the object, you cannot modify or delete the object. Only the application service can modify or delete the object.
- **compression**
  Enables or disables the compression of data according to the methods you select for the attribute **compression-codecs**. The default value is **enabled**.
- **compression-codecs**
  Specifies the codecs to use for compression. The following codecs are available:
  - **bzip2**
    Specifies the use of the bzip2 compression algorithm, which improves compression ratios on low-bandwidth data links.
  - **deflate**
    Specifies the use of the Deflate data compression algorithm.
  - **lzo**
    Specifies the use of the Lempel-Ziv-Oberhumer (LZO) data compression algorithm.
- **data-encryption**
  Enables or disables encryption of the traffic on the outbound connection. If you select **enabled**, the system uses the SSL profiles specified on the local and remote endpoints of the iSession connection. The default value is **disabled**.

- **deduplication**
  Enables or disables data deduplication, which replaces previously transmitted data with references, thus reducing the amount of bandwidth needed to transfer data over the WAN. The default value is **enabled**.
- **defaults-from**
  Specifies the profile that you want to use as the parent profile. The new profile inherits all settings and values from the parent profile specified. The default value is **isession**.
- **deflate-compression-level**
  Specifies the level of compression, if **deflate-compression** is specified and **adaptive-compression** is disabled. The range is **1** to **9**. A higher value causes the CPU to spend more time looking for matches, which may result in better compression. The default value is **1**.
- **description**
  User defined description.
- **glob**
  Displays the items that match the **glob** expression. See **help glob** for a description of **glob** expression syntax.
- **mode**
  Enables or disables the use of this profile for WAN optimization traffic. The default value is **enabled**.
- **name**
  Specifies a unique name for the component. This option is required for the commands **create**, **delete**, and **modify**.
- **partition**
  Displays the administrative partition within which the component resides.
- **port-transparency**
  Enables or disables the preservation of the destination port specified by the client over the WAN. The default value is **enabled**.
- **regex**
  Displays the items that match the regular expression. The regular expression must be preceded by an at sign (@[regular expression]) to indicate that the identifier is a regular expression. See **help regex** for a description of regular expression syntax.
- **reuse-connection**
  Enables or disables the saving and reuse of connections between the local and remote WAN Optimization Managers. The default value is **enabled**.
- **target-virtual**
  For terminated iSession traffic, specifies the matching criteria that a client-side BIG-IP system uses to select a target virtual server on the server-side BIG-IP system.
  The default value is **virtual-match-all**. The options are:
  - **none**
    Specifies that the system sends the terminated iSession traffic directly to the server.

- **host-match-all**
  Specifies that the system selects the closest match from all the host virtual servers.
- **host-match-no-isession**
  Specifies that the system matches only host virtual servers with no iSession profile.
- **virtual-match-all**
  Specifies that the system selects the closest match from all the virtual servers.

See Also

create, *delete*, glob, *list*, *virtual*, *modify*, regex, *reset-stats*, *show*, *tmsh*, *local-endpoint*, *remote-endpoint*

mapi

Configures a Messaging Application Program Interface (MAPI) profile.

Syntax

Configure the **mapi** component within the **wom profile** module using the following syntax.

Create/Modify

```
create mapi [name]
modify mapi [name]
    app-service [[string] | none]
    defaults-from [ [name] | none]
    description [string]
    discover-exchange-servers [disabled | enabled]
    native-compression [disabled | enabled]
```

Display

```
list mapi
list mapi [ [ [name] | [glob] | [regex] ] ... ]
show running-config mapi
show running-config mapi [ [ [name] | [glob] | [regex] ] ... ]
    all-properties
    app-service
    non-default-properties
    one-line
    partition
show mapi
show mapi [ [ [name] | [glob] | [regex] ] ... ]
    (default | exa | gig | kil | meg | peta | raw | tera | yotta | zetta)
```

Delete

```
delete mapi [name]
```

Description

You can use the **mapi** component to manage a MAPI profile.

Examples

create mapi my_mapi_profile

Creates a MAPI profile named **my_mapi_profile** using the system defaults.

modify mapi my_mapi_profile native-compression enabled

Turns on **native-compression** for the MAPI profile named **my_mapi_profile**.

Options

- **app-service**
  Specifies the name of the application service to which the object belongs. The default value is **none**. **Note:** If the **strict-updates** option is **enabled** on the application service that owns the object, you cannot modify or delete the object. Only the application service can modify or delete the object.
- **defaults-from**
  Specifies the profile that you want to use as the parent profile. The new profile inherits all settings and values from the parent profile specified. The default value is **mapi**.
- **description**
  User defined description.
- **discover-exchange-servers**
  Enables or disables the automatic discovery of the Microsoft Exchange servers in the network and creation of a virtual server for each one discovered. The default value is **disabled**.
- **glob**
  Displays the items that match the **glob** expression. See **help glob** for a description of **glob** expression syntax.
- **name**
  Specifies a unique name for the component. This option is required for the commands **create**, **delete**, and **modify**.
- **native-compression**
  Enables or disables native Microsoft Exchange compression. The default value is **disabled**.
- **partition**
  Displays the administrative partition within which the component resides.
- **regex**
  Displays the items that match the regular expression. The regular expression must be preceded by an at sign (@[regular expression]) to indicate that the identifier is a regular expression. See **help regex** for a description of regular expression syntax.

See Also

create, *delete*, glob, *list*, *virtual*, *modify*, regex, *show*, *tmsh*

Glossary

address resolution protocol

Address Resolution Protocol (ARP) is an industry-standard protocol that determines a host's Media Access Control (MAC) address based on its IP address.

administrative partition

An administrative partition is a logical container that you create, containing a defined set of BIG-IP® system objects, such as virtual servers, pools, and profiles. See also *pool*, *profile,* and *virtual server*.

allow list

An allow list displays which service and protocol ports allow connections from outside the system.

ARP

See *address resolution protocol*.

authentication

Authentication is the process of verifying a user's identity when the user is attempting to log in to a system.

authentication profile

An authentication profile is a configuration tool that you use to implement a pluggable authentication module (PAM). Types of authentication modules that you can implement with an authentication profile are: LDAP, RADIUS, TACACS+, SSL Client Certificate LDAP, and OCSP. See also *profile*.

bigdb

Every BIG-IP system includes a bigdb database. The bigdb database holds a set of bigdb configuration keys that define the behavior of various aspects of the BIG-IP system.

certificate

A certificate is an online credential signed by a trusted certificate authority and used for SSL network traffic as a method of authentication. See also *certificate authority (CA)*.

certificate authority (CA)

A certificate authority is an external, trusted organization that issues a signed digital certificate to a requesting computer system for use as a credential to obtain authentication for SSL network traffic. See also *certificate*.

certificate revocation list

A certificate revocation list (CRL) is a list that an authenticating system checks to see if the SSL certificate that the requesting system presents for authentication has been revoked. See also *certificate*.

certificate verification

Certificate verification is the part of an SSL handshake that verifies that a client's SSL credentials have been signed by a trusted certificate authority. See also *certificate*.

chunking

Chunking refers to the HTTP 1.1 feature known as chunked encoding, which allows HTTP messages to be broken up into several parts. Chunking is most often used by servers when sending responses.

class

A class is a list of data that you define and use with iRules® operators. Internal classes are stored in the bigip.conf file. External classes are stored in external files that you define.

client-side SSL profile

A client-side SSL profile is an SSL profile that controls the behavior of SSL traffic going from a client system to the BIG-IP system. See also *profile*.

clone pool

A clone pool replicates all traffic coming into it, and sends that traffic to a duplicate pool. See also *pool*.

configuration object

A configuration object is a user-created object that the BIG-IP system uses to implement a PAM authentication module. There is one type of configuration object for each type of authentication module that you create.

Configuration utility

The Configuration utility is the browser-based application that you use to configure the BIG-IP system.

connection persistence

Connection persistence is an optimization technique whereby a network connection is intentionally kept open for the purpose of reducing handshaking.

cookie persistence

Cookie persistence is a mode of persistence where the BIG-IP system stores persistent connection information in a cookie.

CRL

See *certificate revocation list*.

current partition

When a user logs on, the system determines the default current partition (usually the partition Common) based on the user's logon account. If the user's account grants permission to access more than one partition, the user can change the current partition, and can also change the default current partition. See also *administrative partition*.

custom monitor

A custom monitor is a user-created monitor. See also *monitor*.

custom profile

A custom profile is a user-created profile. A custom profile can inherit its default settings from a parent profile that you specify. See also *profile*.

default-deny policy

A default-deny policy restricts Internet access to everything that is not explicitly permitted.

failover

Failover is the process whereby a standby unit in a redundant system takes over when a software failure or a hardware failure is detected on the active unit. See also *redundant system*.

floating IP address

An IP address assigned to a VLAN and shared between two computer systems is known as a floating IP address. See also *VLAN (virtual local area network)*.

glob matching

glob matching is a pattern matching facility that the tmsh command completion feature uses to complete object identifiers.

hash persistence

Hash persistence allows you to create a persistence hash based on an existing iRule. See also *iRules*.

health monitor

A health monitor checks a node to see if it is up and functioning for a given service. If the node fails the check, it is marked down. Different monitors exist for checking different services. See also *monitor*.

host

A host is a virtual server that represents a specific site, such as an Internet web site or an FTP site, and it load balances traffic targeted to content servers that are members of a pool. See also *virtual server* and *pool*.

HTTP redirect

An HTTP redirect sends an HTTP 302 Object Found message to clients. You can configure a pool with an HTTP redirect to send clients to another node or virtual server if the members of the pool are marked down. See also *virtual server* and *pool*.

HTTP header transformation

When the BIG-IP system performs an HTTP transformation, the system manipulates the Connection header of a server-side HTTP request, to ensure that the connection stays open.

ICMP

See *internet control message protocol*.

interface

A physical port on a BIG-IP system is called an interface.

internal VLAN

The internal VLAN is a default VLAN on the BIG-IP system. In a basic configuration, this VLAN has the administration ports open. In a normal configuration, this is a network interface that handles connections from internal servers. See also *VLAN (virtual local area network)*.

internet control message protocol

Internet Control Message Protocol (ICMP) is an Internet communications protocol used to determine information about routes to destination addresses.

iRules

iRules® are scripts that you write to direct and manipulate the way that the BIG-IP system manages application traffic.

last hop

A last hop is the final hop a connection takes to get to the BIG-IP system. You can allow the BIG-IP system to determine the last hop automatically to send packets back to the device from which they originated. You can also specify the last hop manually by making it a member of a last hop pool. See also *pool*.

Layer 1 through Layer 7

Layers 1 through 7 refer to the seven layers of the Open System Interconnection (OSI) model. Thus, Layer 2 represents the data-link layer, Layer 3 represents the IP layer, and Layer 4 represents the transport layer (TCP and UDP). Layer 7 represents the application layer, handling traffic such as HTTP and SSL.

LDAP

Lightweight Directory Access Protocol (LDAP) is an Internet protocol that email programs use to look up contact information from a server.

LDAP authentication module

An LDAP authentication module is a user-created module that you implement on an BIG-IP system to authenticate client traffic using a remote LDAP server. See also *LDAP*.

LDAP client certificate SSL authentication module

An LDAP client certificate SSL authentication module is a user-created module that you implement on an BIG-IP system to authorize client traffic using SSL client credentials and a remote LDAP server. See also *LDAP*.

link aggregation

The main objective of link aggregation is to provide increased bandwidth at a lower cost, without having to upgrade hardware. The bandwidth of the aggregated trunk is the sum of the capacity of individual member links. Thus it provides an option for linearly incremental bandwidth as opposed to bandwidth options available through physical layer technology. The traffic management system supports link aggregation control protocol (LACP).

load balancing method

A load balancing method is a method of determining how to distribute connections across a load balancing pool. See also *pool*.

local traffic management

Local traffic management is the process of managing network traffic that comes into or goes out of a local area network (LAN), including an intranet.

MAC

Media Access Control (MAC) is a protocol that defines the way workstations gain access to transmission media, and is most widely used in reference to LANs. For IEEE LANs, the MAC layer is the lower sublayer of the data link layer protocol.

MAC address

A MAC address is used to represent hardware devices on an Ethernet network. See also *MAC*.

management interface

The management interface is a special port on the BIG-IP system, used for managing administrative traffic. Named MGMT, the management interface does not forward user application traffic, such as traffic slated for load balancing.

management route

A management route is a route that forwards traffic through the special management (MGMT) interface. See also *management interface*.

MCPD service

The Master Control Program Daemon (MCPD) service manages the configuration data on a BIG-IP system.

MGMT

See *management interface*.

monitor

The BIG-IP system uses monitors to determine whether nodes are up or down. There are several different types of monitors, and they use various methods to determine the status of a server or service.

monitor association

A monitor association is an association that a user makes between a health or performance monitor and a pool, pool member, or node. See also *monitor*.

NAT (network address translation)

A Network Address Translation (NAT) is an alias IP address that identifies a specific node managed by the BIG-IP system to the external network.

network virtual server

A network virtual server is a virtual server whose IP address has no bits set in the host portion of the IP address (that is, the host portion of its IP address is 0). There are two kinds of network virtual servers: those that direct client traffic based on a range of destination IP addresses, and those that direct client traffic based on specific destination IP addresses that the BIG-IP system does not recognize. See also *virtual server*.

node

A node is a logical object on the BIG-IP system that identifies the IP address of a physical resource on the network. Nodes are directly associated with pool members and monitors. See also *pool member* and *monitor*.

node address

A node address is the IP address associated with one or more nodes. This IP address can be the real IP address of a network server, or it can be an alias IP address on a network server.

non-terminated SSL session

A non-terminated SSL session is a session in which the system does not perform the tasks of SSL certificate authentication, encryption, and re-encryption. See also *SSL (Secure Sockets Layer)*.

OCSP (online certificate status protocol)

Online Certificate Status Protocol (OCSP) is a protocol that authenticating systems can use to check on the revocation status of digitally-signed SSL certificates. The use of OCSP is an alternative to the use of a CRL. See also *certificate revocation list*.

OCSP responder

An OCSP responder is an external server used for communicating SSL certificate revocation status to an authentication server such as the BIG-IP system. See also *OCSP (online certificate status protocol)*.

OneConnect

The F5 Networks OneConnect™ feature optimizes the use of network connections by keeping server-side connections open and pooling them for re-use.

packet rate

The packet rate is the number of data packets per second processed by a server.

PAM

A pluggable authentication module (PAM) is a mechanism that integrates multiple low-level authentication schemes into a high-level application programming interface.

partition

See *administrative partition*.

passive failure

A passive failure is a pool member connection failure.

persistence profile

A persistence profile is a pre-configured object that automatically enables persistence when you assign the profile to a virtual server. See also *profile*.

pluggable authentication module

See *PAM*.

pool

A pool is composed of a group of network devices (called members). The BIG-IP system load balances requests to the nodes within a pool based on the load balancing method and persistence method you choose when you create the pool or edit its properties.

pool member

A pool member is a server that is a member of a load balancing pool. See also *pool*.

pre-configured monitor

A pre-configured monitor is a monitor that the BIG-IP system provides. See also *monitor*.

profile

A profile is a configuration tool containing settings for defining the behavior of network traffic. The BIG-IP system contains profiles for managing FastL4, HTTP, TCP, FTP, SSL, and RTSP traffic, as well as for implementing persistence and application authentication.

Quality of Service (QoS) level

The Quality of Service (QoS) level is a means by which network equipment can identify and treat traffic differently based on an identifier. Essentially, the QoS level specified in a packet enforces a throughput policy for that packet. See also *type of service (ToS) level*.

rate class

A rate class determines the volume of traffic allowed through a rate filter.

rate shaping

Rate shaping is a type of extended IP filter. Rate shaping uses the same IP filter method but applies a rate class, which determines the volume of network traffic allowed.

redundant system

A redundant system is a pair of units that are configured for fail-over. Of the two units, one is running as the active unit and one is running as the standby unit. If the active unit fails, the standby unit takes over and manages connection requests.

source address translation

Source address translation is the process of converting a source address in an IP packet to some other address, so that it appears that the packet originated from a different device. You can configure source address translation to convert many addresses to a single address, or to convert a particular source address.

SCF (single configuration file)

An SCF is a flat, text file with an extension of .scf that contains the configuration of a BIG-IP system.

self IP address

A self IP address is an IP address that is assigned to the system. Self IP addresses are part of the base configuration. You must define at least one self IP address for each VLAN.

SIP persistence

SIP persistence is a type of persistence used for servers that receive Session Initiation Protocol (SIP) messages sent through UDP. SIP is a protocol that enables real-time messaging, voice, data, and video.

SNAT (secure network address translation)

A SNAT is a feature you can configure on the BIG-IP system. A SNAT defines a routable alias IP address that one or more nodes can use as a source IP address when making connections to hosts on the external network.

SNAT pool

SNAT pool is a pool of translation addresses that you can map to one or more original IP addresses. Translation addresses in a SNAT pool are not self IP addresses. See also *pool*.

spanning tree protocol (STP)

Defined by IEEE, Spanning Tree Protocol (STP) is a protocol that provides loop resolution in configurations where one or more external switches are connected in parallel with the BIG-IP system.

SSH

SSH (secure shell) is a protocol for secure remote logon and other secure network services over a non-secure network.

SSL (Secure Sockets Layer)

Secure Sockets Layer (SSL) is a network communications protocol that uses public-key technology as a way to transmit data in a secure manner.

SSL persistence

SSL persistence is a type of persistence that tracks non-terminated SSL sessions, using the SSL session ID. See also *SSL (Secure Sockets Layer)*.

SSL profile

An SSL profile is a configuration tool that you use to initiate and end SSL connections from clients and servers. See also *SSL (Secure Sockets Layer)* and *profile*.

TACACS

Terminal Access Controller Access Control System (TACACS) is an older authentication protocol common to UNIX® systems. TACACS allows a remote access server to forward a user's logon password to an authentication server.

TACACS+

TACACS+ is an authentication mechanism designed as a replacement for the older TACACS protocol. There is little similarity between the two protocols, however, and they are therefore not compatible. See also *TACACS*.

Tcl

See *Tools Command Language*.

TMM service

See *Traffic Management Microkernel Service*.

Tools Command Language

Tools Command Language (Tcl) is an industry-standard scripting language. On the BIG-IP system, users use Tcl to write iRules. See also *iRules.*

topology statement

A topology statement is a set of characteristics that identify the origin of a given name resolution request.

ToS level

See *type of service (ToS) level.*

Traffic Management Microkernel Service

The Traffic Management Microkernel (TMM) service is the process running on the BIG-IP system that performs most traffic management for the product.

trunking

Trunking is link aggregation that allows multiple physical links to be treated as one logical link. See also *link aggregation*.

trusted CA file

A trusted CA file is a file containing a list of certificate authorities that an authenticating system can trust when processing client requests for authentication. A trusted CA file resides on the authenticating system and is used for authenticating SSL network traffic. See also *certificate authority*.

trusted MAC address

A trusted MAC address is a MAC address that passes MAC address-based authentication. See also *MAC address*.

type of service (ToS) level

The Type of Service (ToS) level is another means, in addition to the QoS level, by which network equipment can identify and treat traffic differently based on an identifier. See also *Quality of Service (QoS) level*.

UCS (user configuration set)

A UCS is an archive of all of the BIG-IP system configuration files stored in a file with an extension of .ucs.

user role

A user role is a type and level of access that you assign to a BIG-IP system user account. By assigning user roles, you can control the extent to which BIG-IP system administrators can view or modify the BIG-IP system configuration.

vCMP

Virtualized Clustered Multiprocessing (vCMP) is a feature of the BIG-IP system that allows you to run multiple instances of the BIG-IP software on a single F5 Networks hardware platform.

virtual address

A virtual address is an IP address associated with one or more virtual servers managed by the BIG-IP system.

virtual server

A virtual server is a specific combination of virtual address and virtual port, associated with a content site that is managed by an BIG-IP system or other type of host server.

VLAN (virtual local area network)

A VLAN is a logical grouping of interfaces connected to network devices. You can use a VLAN to logically group devices that are on different network segments. Devices within a VLAN use Layer 2 networking to communicate and define a broadcast domain.

VLAN group

A VLAN group is a logical container that includes two or more distinct VLANs. VLAN groups are intended for load balancing traffic in a Layer 2 network, when you want to minimize the reconfiguration of hosts on that network. See also *VLAN (virtual local area network)*.

Index

A

aaa-active-directory component 35-2
aaa-client-cert component 35-5
aaa-crldp component 35-7
aaa-http component 35-9
aaa-ldap component 35-11
aaa-ocsp component 35-16
aaa-radius component 35-18
aaa-securid component 35-20
access component 36-2
access-policy component 34-2
acct-radius component 35-22
acct-tacacsplus component 35-24
acl component 28-2
action component 80-2
active-directory component 29-2
active-directory-trusted-domains component 29-5
address-list component 85-2
admin-partitions component 43-2
ad-policy component 112-2
advertised-route component 114-2
alertd component 101-2
alg-log-profile component 49-2
all-stats component 102-2
analytics application-security module 5-1
analytics application-security-network module 6-1, 7-1
analytics component 67-2, 76-2
analytics cpu module 8-1
analytics disk-info module 9-1
analytics dns module 10-1
analytics dns-dos module 11-1
analytics dns-protocol module 12-1
analytics dos-l3 module 13-1
analytics dos-l7 module 14-1
analytics http module 15-1
analytics ip-layer module 16-1
analytics memory module 17-1
analytics module 4-1
analytics network module 18-1
analytics pem module 19-1
analytics protocol-security module 20-1
analytics sip-dos module 21-1
analytics swg module 22-1
analytics swg-blocked module 23-1
analytics tcp module 24-1
analytics udp module 25-1
analytics vcmp module 26-1
analytics virtual module 27-1
apache-ssl-cert component 95-2
apl-script component 90-2
apm aaa module 29-1
apm epsec module 30-1
apm mam module 31-1
apm mam scim-config module 32-1
apm module 28-1
apm ntlm module 33-1
apm policy agent module 35-1
apm policy module 34-1
apm profile module 36-1
apm resource module 37-1
apm resource remote-desktop module 38-1
apm saml module 39-1
apm sso module 40-1
apm-auth component 42-2
apm-avr-config component 28-6
application component 51-2, 52-2, 112-4
application-volume component 94-2
app-tunnel component 37-2
arcsight component 101-4
arp component 68-2
array component 103-2
artifact-resolution-service component 39-2
asm module 41-1
audit entries table 2-15
audit file 2-15
audit log 2-15
auth module 42-1

B

base configuration, saving and loading 2-2
basic component 40-2
batch mode 2-23
bay component 103-4
bigip component 48-2
bigip-link component 48-6
bigstart command 1-2
bigtop utility, defined 1-2
blacklist-category component 87-2
block-device-image component 107-2
block-device-software-hotfix component 107-6
bwc-policy component 68-5
by-handle component 92-2

C

cached-certs component 54-2
category component 51-4
ccmode component 109-2
cd component 3-2
cert component 45-2, 91-2
certificate-authority component 67-11
cert-ldap component 42-4
check-cert component 91-5
cifs component 115-2
citrix component 38-2
citrix-client-bundle component 38-5
citrix-client-package-file component 38-7
class component 73-2
classification component 67-13
cli alias module 44-1
cli module 43-1
client component 91-7

client-ldap component 67-15
client-rate-class component 37-5
client-ssl component 67-17
client-traffic-classifier component 37-8
clock component 89-2
cluster component 89-3
clusterd component 93-2
cm module 45-1
cmetrics component 68-14
command alias 2-17
command audit 2-15
command completion feature 2-7
command history feature 2-11
command line utilities 1-2
command syntax
    global commands 3-1
commands
    about global 3-1
    See specific command name.
component mode, leaving 2-6
components
    navigating out of 2-6
    navigating to 2-1
    working within 2-4
    See individual component name.
concat-set component 113-2
config component 89-5
config utility
    using to set up the BIG-IP system 1-2
config-diff component 89-11
config-sync component 45-5
connection component 61-2, 89-12
connections component 102-4
connectivity component 36-9
console component 89-15
context-sensitive help 2-10
cookie component 66-2
cp component 3-4
cpu component 89-16
create component 3-6
crl component 91-9
crldp component 29-7
crldp-server component 50-2
csyncd component 93-4
customization-group component 34-3
custom-stat component 90-5

D

daemon-ha component 89-17
datacenter component 46-2
data-group component 95-5
datastor component 89-20
db component 89-22
decision-box component 35-26
deduplication component 114-5
default-config component 89-25
default-node-monitor component 49-5
delete component 3-7
dest-addr component 66-6
destination component 99-2
device component 45-7
device-config component 84-2
device-group component 45-11
device-stats component 83-2
device-sync component 41-2
dhcpv4 component 67-30
dhcpv6 component 67-36
diagnose-conn component 114-7
diameter component 65-2, 67-41
diameter-endpoint component 77-2
directory component 94-4
disk component 103-6
distributed-app component 46-5
dnat component 109-3
dns component 65-7, 67-46, 89-26
dns-express-db component 56-2
dns-logging component 67-50
domain-list component 112-10, 113-4
download-result component 108-2
download-schedule component 108-3
drop-policy component 73-6
dynamic-acl component 35-28

E

edit component 3-9
element component 99-3
ending-allow component 35-30
ending-deny component 35-32
ending-redirect component 35-34
endpoint-check-machine-cert component 35-36
endpoint-check-software component 35-39
endpoint-discovery component 114-8
endpoint-linux-check-file component 35-44
endpoint-linux-check-process component 35-47
endpoint-mac-check-file component 35-50
endpoint-mac-check-process component 35-53
endpoint-machine-info component 35-55
endpoint-windows-browser-cache-cleaner component 35-57
endpoint-windows-check-file component 35-60
endpoint-windows-check-process component 35-63
endpoint-windows-check-registry component 35-66
endpoint-windows-info-os component 35-71
endpoint-windows-protected-workspace component 35-73
epsec-package component 30-2
etherip component 74-2
event component 97-2
eviction-policy component 49-7
exchange component 36-14

exit component 3-11
external component 48-9, 55-2, 65-13
external-hsm component 92-3
external-logon-page component 35-75
external-monitor component 95-8

F

failover component 89-28
failover-status component 45-15
fasthttp component 67-53
fastl4 component 67-58
feature-module component 89-31
fec component 74-4
feed-list component 87-4
file-type component 86-2
filter component 100-2
firepass component 48-12, 65-17
firmware-config component 96-2
fix component 67-65
fix-connection component 89-33
folder component 89-34
format-script component 79-2
form-based component 40-5
form-basedv2 component 40-8
forwarding-endpoint component 75-2
ftp component 48-16, 65-21, 67-68

G

gateway-icmp component 48-20, 65-26
gencert utility, defined 1-2
general component 47-2, 61-4
generate component 3-12
generation component 60-2
geoip component 89-37
glob 2-8
glob matching 2-8
global component 110-2
global-policy component 87-8
global-profile component 83-3
global-rules component 85-5
global-settings component 43-3, 57-2, 58-2, 66-10, 69-2, 89-38
gre component 74-7
grep 2-22
gtm component 102-5
gtm global-settings module 47-1
gtm module 46-1
gtm monitor module 48-1
gtp component 48-23
guest component 110-3
gx component 80-5
gy component 80-8

H

ha-group component 89-43
hardware component 89-47
hash component 66-12
ha-status component 89-46, 111-2
help
    using context-sensitive 2-10
help component 3-13
historical logs 2-17
history 2-11
history component 43-5
history feature, for commands 2-11
host-info component 89-48
hotfix component 107-9
hsl component 80-11
html component 67-71
http component 29-10, 48-26, 65-30, 67-74, 105-2, 106-2
http2 component 67-89
httpclass-asm component 41-5
http-compression component 67-84
httpd component 89-49
http-method component 41-3
https component 48-30, 65-36
http-signature component 51-6
hypervisor-info component 89-55

I

icap component 67-92
icmp component 65-42
icmp-stat component 89-56
icrd component 93-6
idbridge component 31-2
ifile component 49-13, 95-10
iiop component 67-95
ike-daemon component 72-2
ike-evt-stat component 68-16
ike-msg-stat component 68-17
ike-peer component 72-4
ike-sa component 72-9
image component 107-12
image-file component 34-4
imap component 48-34, 65-46
inband component 65-50
info component 87-10, 96-4
install component 3-15
interception-endpoint component 75-6
interface component 68-18, 105-3, 106-4
interface-cos component 68-24
internal component 55-6
ip-address component 89-57
ipfix component 101-6
ipip component 74-10
ipother component 67-98
iprep-status component 89-60

ipsec component 74-12
ipsec-policy component 72-10
ipsec-sa component 72-14
ip-stat component 89-59
ipv6-leasepool component 37-11
iquery component 46-9
irule component 75-8
irule-event component 35-77
irules component 99-6
isession component 115-5
istats-trigger component 97-4

K

kerberos component 29-14, 35-79, 40-17
kerberos-delegation component 50-5
kerberos-keytab-file component 29-16
key component 45-16, 51-9, 59-2, 60-4, 91-11, 92-4
keyboard map feature
    and default settings 2-13
    using 2-13

L

ldap component 29-18, 42-9, 48-38, 50-8, 65-53
ldns component 46-10
leasepool component 37-13
license component 89-62
lind component 93-8
link component 46-11
list component 3-16
listener component 46-16, 75-11
load component 3-19
load-balancing component 47-6
loading the system configuration 2-2
local-database component 101-9
local-endpoint component 114-11
local-profile component 83-6
local-syslog component 101-11
log component 89-64
log entries
    for audit 2-15
    for history 2-17
logging component 35-81
logical-disk component 94-5
login-failures component 42-14
logon-page component 35-83
log-rotate component 89-66
log-setting component 28-7
lsndb component 109-5
lsn-log-profile component 49-15
lsn-pool component 49-18
ltm auth module 50-1
ltm classification module 51-1
ltm clientssl module 53-1
ltm clientssl-proxy module 54-1
ltm data-group module 55-1
ltm dns analytics module 57-1
ltm dns cache module 58-1
ltm dns cache records module 59-1
ltm dns dnssec module 60-1
ltm dns module 56-1
ltm message-routing generic module 62-1, 64-1
ltm message-routing sip module 63-1
ltm module 49-1

M

mac-address component 89-69
machine-account component 33-2
mam-server component 31-4
man pages 2-9
management-dhcp component 89-71
management-ip component 89-73
management-ip-rules component 85-14
management-route component 89-75
mandatory-header component 86-3
manual-security-association component 72-16
map component 74-14
map-8021p component 69-4
map-dscp component 69-6
mapi component 115-9
master-key component 91-15
matching-rule component 85-22
mblb component 67-100
mcpd component 93-10
mcp-state component 89-78
memory component 89-79
message-box component 35-87
metrics component 47-8
metrics-exclusions component 47-11
modify component 3-20
module
    leaving 2-6
    navigating to 2-3
    working within 2-3
module-provision component 111-3
module-score component 65-58
msg component 59-4
msrdp component 66-16
mssql component 48-42, 65-62, 67-103
mv component 3-22
mysql component 48-46, 65-67

N

nameserver component 56-3, 59-6
nat component 49-25
ndp component 68-25
net ipsec module 72-1
net tunnels module 74-1
network-access component 37-15
network-storage-field component 88-2
network-whitelist component 84-10

nntp component 48-50, 65-72
node component 49-28
ntlm component 67-106
ntlm-auth component 33-5
ntlmv1 component 40-21
ntlmv2 component 40-24
ntp component 89-80

O

oam component 29-22, 35-89
object mode
    leaving 2-6
    working in 2-5
object-type component 112-12
ocsp component 29-26
ocsp-responder component 50-13
ocsp-stapling-params component 67-109
ocsp-stapling-responses component 53-2
one-connect component 67-112
Openssl utility 1-2
oracle component 48-54, 65-76
outbound-smtp component 89-84

P

packet-filter component 68-27
packet-filter-trusted component 68-32
partition component 42-16
password component 42-18
password-policy component 42-19
path component 46-22
pcp component 67-116
peer component 62-2, 63-2
PEM global-settings module 76-1
PEM module 75-1
PEM profile module 77-1
PEM quota management module 78-1
PEM reporting module 79-1
PEM stats module 80-1
periodic component 98-2
perpetual component 98-5
persist component 46-23
persist-records component 66-19
pkcs12 component 91-17
platform_check component 109-8
policy component 41-7, 49-33, 51-11, 75-13, 85-23, 87-12, 112-15
policy-item component 34-5
policy-strategy component 49-44
pool component 46-25, 49-48
pop3 component 48-58, 65-81
portal-access component 37-23
port-list component 85-28
port-mirror component 68-35
postgresql component 48-61, 65-85
ppp component 74-16
pptp component 67-120
predefined-policy component 41-11
preference component 43-6
preferences
    for show-aliases 2-18
    for statistics 2-19
private component 44-2
prober-pool component 46-37
proc-info component 89-86
profile component 50-18, 82-2, 84-14, 86-4, 88-3
prompt component 111-4
protocol component 62-4
protocol-dns-storage-field component 88-18
protocol-sip-storage-field component 88-19
provision component 89-87
publish component 3-24
publisher component 97-6, 100-5
pva-traffic component 89-91
pwd component 3-25

Q

qoe component 67-122
quest component 38-9
queue component 73-9
quit component 3-26
quota-mgmt component 76-4

R

radius component 29-30, 42-22, 48-65, 50-21, 65-90, 67-124, 80-13
radius-aaa component 77-5
radius-accounting component 48-69, 65-94
radius-server component 42-25, 50-24
ramcache component 67-127, 102-6
rating-group component 78-2
rdp component 38-12
real-server component 48-73, 65-98
reboot component 3-27
receiver component 104-2
region component 46-41
remote-desktop component 36-17
remote-endpoint component 114-14
remote-format component 88-20
remote-high-speed-log component 101-13
remote-role component 42-28
remote-route component 114-19
remote-syslog component 101-15
remote-user component 42-32
report component 4-2, 5-2, 6-2, 7-2, 8-2, 9-2, 10-2, 11-2, 12-2, 13-2, 14-2, 15-2, 16-2, 17-2, 18-2, 19-2, 20-2, 21-2, 22-2, 23-2, 24-2, 25-2, 26-2, 27-2
request-adapt component 67-129
request-log component 67-132
reset-stats component 3-29
resolver component 58-4, 70-2

resource-assign component 35-91
response-adapt component 67-136
response-code component 41-12
restart component 3-31
rewrite component 67-139
rewrite-rule component 95-12
roi-statistics component 112-42
root module
about 2-3
working within 2-3
route component 62-6, 63-4, 68-37
route-domain component 68-40
route-domain-selection component 35-93
router component 62-8, 64-2
router-advertisement component 68-47
rpc component 65-101
rrset component 59-8
rst-cause component 68-51
rtsp component 67-144
rule component 46-44, 49-60
rule-list component 85-31
rule-stat component 85-40
run component 3-32
running configuration 2-2

S

saml component 29-33, 40-27
saml-idp-connector component 29-37
saml-resource component 40-31
saml-sp-connector component 40-33
sandbox component 37-26
sasp component 65-105
save component 3-35
saving the running configuration 2-2
schedule component 85-41
scheduled-report component 5-7
scim-config component 32-2
script component 43-12, 97-7
scriptd component 89-93
scripted component 48-76, 65-108
scripting feature
about 2-6
sctp component 67-148
securid component 29-41
security analytics module 81-1
security anti-fraud module 82-1
security datasync module 83-1
security dos module 84-1
security firewall module 85-1
security http module 86-1
security ip-intelligence module 87-1
security log module 88-1
self component 68-52
self-allow component 68-59
send-mail component 3-36
server component 46-47, 91-19
server-discovery component 114-20
server-ldap component 67-152
server-ssl component 67-154
service component 89-95, 90-7
service-chain-endpoint component 75-24
session component 64-5
sessiondb component 75-28
settings component 81-2
shaping-policy component 73-12
shared component 44-5
show component 3-37
shutdown component 3-41
signature component 107-15
signature-definition component 51-13
signatures component 51-19
signature-update-schedule component 51-15
signature-version component 51-17
sip component 48-79, 65-112, 66-22, 67-164
sipdb component 109-9
smb component 65-117
smtp component 48-84, 65-121, 67-169
smtps component 67-171
smtp-server component 89-97
snat component 49-64
snatpool component 49-71
snat-translation component 49-68
sniff-updates component 45-19
snmp component 48-87, 89-99
snmp-dca component 65-125
snmp-dca-base component 65-129
snmp-link component 48-91
soap component 48-95, 65-132
socks component 67-173
software component 111-5
software-status component 30-4
source component 42-34
source-addr component 66-25
spdy component 67-176
special characters 2-25
splunk component 101-18
spm component 77-7
sshd component 89-113
ssh-keyswap component 109-11
ssl component 66-29
ssl-cc-ldap component 50-27
ssl-cert component 95-14
ssl-crl component 95-17
ssl-crldp component 50-32
ssl-key component 95-19
ssl-ocsp component 50-35
stale-rules component 18-10
start component 3-42
state-mirroring component 89-116
statistics component 67-180
statistics feature

resetting 2-22
using 2-19
statistics, viewing 2-19
status component 107-17
stop component 3-43
storage-field component 88-22
stored configuration files 2-2
stp component 68-61
stp-globals component 68-65
stream component 67-183
submit component 3-44
subscriber component 75-31, 80-15
subscriber-activity-log component 76-6
subscribers component 75-34
swg-scheme component 28-9
sync-status component 45-20
sync-sys-files component 89-118
syntax conventions 1-3
sys application module 90-1
sys crypto fips module 92-1
sys daemon-log-settings module 93-1
sys disk module 94-1
sys file module 95-1
sys fpga module 96-1
sys icall handler module 98-1
sys icall module 97-1
sys ipfix module 99-1
sys log-config destination module 101-1
sys log-config module 100-1
sys module 89-1
sys sflow data-source module 105-1
sys sflow global-settings module 106-1
sys sflow module 104-1
sys software module 107-1
sys url-db module 108-1
syslog component 89-119
system component 102-7, 105-4, 106-6
system configuration, loading and saving 2-2

T

tacacs component 42-36, 50-38
tacacsplus component 29-43, 35-95
Tcl, defined 1-2
tcp component 48-99, 65-137, 67-186
tcp-echo component 65-142
tcp-half-open component 48-103, 65-146
template component 90-10
test-monitor component 109-12
throughput component 102-8
time component 3-45
tm profile module 52-1, 67-1
tmm component 93-12
tmm-info component 89-123
tmm-traffic component 89-124
TMOS 1-1
tmsh
and command completion 2-7
and command history 2-11
and command syntax 2-2
and modular structure 2-1
closing 2-6
introducing 1-1
tmsh component 3-48
tmsh hierarchy
understanding 2-1
working within 2-3
tmsh modules, working with 2-1
tmsh prompt 2-2
Tools Command Language 1-2
topology component 46-55
tracepath component 109-13
tracepath6 component 109-14
traceroute component 109-15
traceroute6 component 109-16
traffic component 46-58, 89-125
Traffic Management Operating System 1-1
Traffic Management Shell
See tmsh.
traffic-class component 49-73
traffic-control component 61-6
traffic-group component 45-21
traffic-priority component 69-8
traffic-selector component 72-19
transaction component 43-31
transparent component 58-10
transport-config component 62-11, 63-7
triggered component 98-8
trunk component 68-68
trust-domain component 45-24
tsig-key component 56-5
tunnel component 71-2, 74-19

U

ucs component 89-126
udp component 48-106, 65-150, 67-196
udp-portlist component 84-28
universal component 66-32
update component 107-19
update-signatures component 51-20
update-status component 107-21
url component 113-6
url-category component 51-21, 52-4, 108-5
urldb-feed-list component 51-23
urldb-file component 51-25
url-filter component 28-11
user component 42-39
user-domain component 85-44
user-list component 85-46

V

v6rd component 74-22
validating-resolver component 58-14
variable-assign component 35-97
vconsole component 109-17
vdi component 36-18
vdisk component 110-8
verify-config component 114-23
version component 43-34, 89-128
virtual component 49-76
virtual-address component 49-89
virtual-disk component 110-9
virtual-disk-template component 110-10
virtual-location component 65-156
vlan component 68-73, 71-4, 105-5, 106-8
vlan-allowed component 68-78
vlan-group component 68-79
vmware-view component 38-18
volume component 107-23
vxlan component 74-25

W

wa-cache component 67-199
wam module 112-1
wam resource module 113-1
wap component 48-110, 65-160
Warning
    This page is obsolete. Windows Group Policy is no longer supported. 34-6, 35-69
watch-devicegroup-device component 45-28
watch-sys-device component 45-30
watch-trafficgroup-device component 45-32
wccp component 68-83, 74-27
web-acceleration component 67-200
webapp-language component 41-14
web-security component 67-204
webtop component 37-29
webtop-link component 37-32
wideip component 46-59
wildcard search 2-19
wmi component 48-114, 65-165
wom module 114-1
wom profile module 115-1

X

xml component 67-206

Z

zebos component 109-18
zone component 56-7, 60-8