External Monitoring of BIG-IP® Systems: Implementations

Version 11.6

Table of Contents

Legal Notices and Acknowledgments....11
Legal Notices....11
Acknowledgments....12

Configuring Request Logging....25
Overview: Configuring a Request Logging profile....25
Creating a pool with request logging to manage HTTP traffic....25
Creating a request logging profile....26
Configuring a virtual server for request logging....27
Deleting a request logging profile....28
Request Logging profile settings....28
Request Logging parameters....30

Configuring Remote High-Speed Logging of BIG-IP System Processes....33
Overview: Configuring high-speed remote logging of BIG-IP system processes....33
Creating a pool of remote logging servers....34
Creating a remote high-speed log destination....35
Creating a formatted remote high-speed log destination....35
Creating a publisher 36
Creating a logging filter....36
Disabling system logging 37
Troubleshooting logs that contain unexpected messages 37

Configuring Remote High-Speed DNS Logging....39
Overview: Configuring remote high-speed DNS logging....39
Creating a pool of remote logging servers....40
Creating a remote high-speed log destination....41
Creating a formatted remote high-speed log destination....41
Creating a publisher 42
Creating a custom DNS logging profile for logging DNS queries 42
Creating a custom DNS logging profile for logging DNS responses....43
Creating a custom DNS logging profile for logging DNS queries and responses 43
Creating a custom DNS profile to enable DNS logging 44
Configuring a listener for DNS logging....44
Configuring an LTM virtual server for DNS logging....45
Disabling DNS logging 45
Implementation result....45

Configuring Remote High-Speed Logging of Protocol Security Events.....47
Overview: Configuring Remote Protocol Security Event Logging.....47
Creating a pool of remote logging servers.....48
Creating a remote high-speed log destination.....49
Creating a formatted remote high-speed log destination.....49
Creating a publisher 50
Creating a custom Protocol Security Logging profile 50
Configuring a virtual server for Protocol Security event logging.....51
Disabling logging 52
Implementation result.....52

Configuring Remote High-Speed Logging of Network Firewall Events.....53
Overview: Configuring remote high-speed Network Firewall event logging.....53
Creating a pool of remote logging servers.....54
Creating a remote high-speed log destination.....55
Creating a formatted remote high-speed log destination.....55
Creating a publisher 56
Creating a custom Network Firewall Logging profile 56
Configuring a virtual server for Network Firewall event logging.....58
Disabling logging 58
Implementation result.....59

Configuring Remote High-Speed Logging of DoS Protection Events.....61
Overview: Configuring DoS Protection event logging.....61
Creating a pool of remote logging servers.....62
Creating a remote high-speed log destination.....63
Creating a formatted remote high-speed log destination.....63
Creating a publisher 64
Creating a custom DoS Protection Logging profile 64
Configuring an LTM virtual server for DoS Protection event logging.....65
Disabling logging 65
Implementation result.....66

Configuring Remote High-Speed Logging of CGNAT Processes.....67
Overview: Configuring remote high-speed logging for CGNAT.....67
Creating a pool of remote logging servers.....68
Creating a remote high-speed log destination.....69
Creating a formatted remote high-speed log destination.....69
Creating a publisher 70
Creating an LSN logging profile.....70
Configuring an LSN pool 71

Configuring CGNAT IPFIX Logging....73
Overview: Configuring IPFIX logging for CGNAT....73
Assembling a pool of IPFIX collectors....74
Creating an IPFIX log destination....75
Creating a publisher....75
Creating an LSN logging profile....76
Configuring an LSN pool....76

Logging Network Firewall Events to IPFIX Collectors....79
Overview: Configuring IPFIX logging for AFM....79
Assembling a pool of IPFIX collectors....79
Creating an IPFIX log destination....80
Creating a publisher....81
Creating a custom Network Firewall Logging profile....81
Configuring an LTM virtual server for Network Firewall event logging with IPFIX....82
Implementation result....83

Customizing IPFIX Logging with iRules....85
Overview: Customizing IPFIX logging with iRules....85
Assembling a pool of IPFIX collectors....86
Creating an IPFIX log destination....87
Creating a publisher....87
About standard IPFIX elements....88
Writing an iRule for custom IPFIX logging....88
Adding the iRule to a virtual server....90
Showing IPFIX statistics....91
Advanced IPFIX iRule tasks....92
Implementation result....95

Monitoring BIG-IP System Traffic with SNMP....97
Overview: Configuring network monitoring using SNMP....97
SNMP deployment worksheet....97
Component overview....98
Permissions on SNMP data objects....98
About enterprise MIB files....98
Downloading enterprise and NET-SNMP MIBs to the SNMP manager....99
Viewing objects in enterprise MIB files....100
Viewing SNMP traps in F5-BIGIP-COMMON-MIB.txt....100
Viewing dynamic routing SNMP traps and associated OIDs....100
Monitoring BIG-IP system processes using SNMP....100
Collecting BIG-IP system memory usage data using SNMP....101

Collecting BIG-IP system data on HTTP requests using SNMP....101
Collecting BIG-IP system data on throughput rates using SNMP....102
Collecting BIG-IP system data on RAM cache using SNMP....103
Collecting BIG-IP system data on SSL transactions using SNMP....104
Collecting BIG-IP system data on CPU usage based on a predefined polling interval....105
Collecting BIG-IP system data on CPU usage based on a custom polling interval....106
Collecting BIG-IP system performance data on new connections using SNMP....107
Collecting BIG-IP system performance data on active connections using SNMP....108
About the RMON MIB file....109
About customized MIB entries....109
Creating custom MIB entries....110
Overview: BIG-IP SNMP agent configuration....111
Specifying SNMP administrator contact information and system location information....111
Configuring SNMP manager access to the SNMP agent on the BIG-IP system....111
Granting community access to v1 or v2c SNMP data....112
Granting user access to v3 SNMP data....112
Overview: SNMP trap configuration....113
Enabling traps for specific events....113
Setting v1 and v2c trap destinations....114
Setting v3 trap destinations....114
Viewing pre-configured SNMP traps....115
Creating custom SNMP traps....115
Overview: About troubleshooting SNMP traps....116
AFM-related traps and recommended actions....116
ASM-related traps and recommended actions....117
Application Visibility and Reporting-related traps and recommended actions....118
Authentication-related traps and recommended actions....118
DoS-related traps and recommended actions....119
General traps and recommended actions....119
GTM-related traps and recommended actions....119
Hardware-related traps and recommended actions....122
High-availability system-related traps and recommended actions....126
License-related traps and recommended actions....127
LTM-related traps and recommended actions....128
Logging-related traps and recommended actions....129
Network-related traps and recommended actions....129
vCMP-related traps and recommended actions....130
VIPRION-related traps and recommended actions....130

Monitoring BIG-IP System Traffic with sFlow....131
Overview: Configuring network monitoring with sFlow....131
Adding a performance monitoring sFlow receiver....131
Setting global sFlow polling intervals and sampling rates for data sources....132
Setting the sFlow polling interval and sampling rate for a VLAN....132
Setting the sFlow polling interval and sampling rate for a profile....132
Setting the sFlow polling interval for an interface....133
Viewing sFlow data sources, polling intervals, and sampling rates....133
sFlow receiver settings....134
sFlow global settings....134
sFlow counters and data....134
sFlow HTTP Request sampling data types....137
sFlow VLAN sampling data types....140
Implementation result....143

Event Messages and Attack Types....145
Fields in ASM Violations event messages....145
ASM Violations example events....146
Fields in ASM Brute Force and Web Scraping event messages....148
ASM Anomaly example events....150
Fields in AFM event messages....151
AFM example events....152
Fields in Network DoS Protection event messages....154
Device DoS attack types....155
Network DoS Protection example events....161
Fields in Protocol Security event messages....163
Protocol Security example events....163
Fields in DNS event messages....165
DNS attack types....166
DNS example events....167
Fields in DNS DoS event messages....168
DNS DoS attack types....169
DNS DoS example events....170
BIG-IP system process example events....170

IPFIX Templates for CGNAT Events....171
Overview: IPFIX logging templates....171
IPFIX information elements for CGNAT events....171
IANA-Defined IPFIX information elements....171
IPFIX enterprise information elements....172
Individual IPFIX templates for each event....172
NAT44 session create – outbound variant....173
NAT44 session delete – outbound variant....173

NAT44 session create – inbound variant....174
NAT44 session delete – inbound variant....175
NAT44 translation failed....176
NAT44 quota exceeded....176
NAT44 port block allocated or released....177
NAT64 session create – outbound variant....177
NAT64 session delete – outbound variant....178
NAT64 session create – inbound variant....179
NAT64 session delete – inbound variant....179
NAT64 translation failed....180
NAT64 quota exceeded....181
NAT64 port block allocated or released....181
DS-Lite session create – outbound variant....182
DS-Lite session delete – outbound variant....182
DS-Lite session create – inbound variant....183
DS-Lite session delete – inbound variant....184
DS-Lite translation failed....185
DS-Lite quota exceeded....185
DS-Lite port block allocated or released....186

IPFIX Templates for AFM Events....187
Overview: IPFIX Templates for AFM Events....187
About IPFIX Information Elements for AFM events....187
IANA-defined IPFIX Information Elements....187
IPFIX enterprise Information Elements....187
About individual IPFIX templates for each event....189
Network accept or deny....189
DoS device....190
IP intelligence....191
Log Throttle....193

IPFIX Templates for AFM DNS Events....195
Overview: IPFIX Templates for AFM DNS Events....195
About IPFIX Information Elements for AFM DNS events....195
IANA-defined IPFIX Information Elements....195
IPFIX enterprise Information Elements....195
About individual IPFIX Templates for each event....196
IPFIX template for DNS security....196
IPFIX template for DNS DoS....197

IPFIX Templates for AFM SIP Events....199
Overview: IPFIX Templates for AFM SIP Events....199
About IPFIX Information Elements for AFM SIP events....199
IANA-defined IPFIX information elements....199

IPFIX enterprise Information Elements....199
About individual IPFIX Templates for each event....200
IPFIX template for SIP security....200
IPFIX template for SIP DoS....201

Legal Notices and Acknowledgments

Legal Notices

Publication Date

This document was published on November 11, 2016.

Publication Number

MAN-0530-00

Copyright

Copyright © 2014-2016, 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 ICES-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:

a. copy, modify, rent, sell, distribute or transfer any part of the Software, and You agree to prevent unauthorized copying of the Software; and,

b. reverse engineer, decompile, or disassemble the Software; and,

c. sublicense or permit simultaneous use of the Software by more than one user; and,

d. otherwise assign, sublicense, lease, or in any other way transfer or disclose Software to any third party, except as set forth herein; and,

e. 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:

  a. be disclosed or distributed in source code form; or

  b. be licensed by the user to third parties for the purpose of making and/or distributing derivative works; or

  c. 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:

a. GNU's General Public License (GPL) or Lesser/Library GPL (LGPL),

b. the Artistic License (e.g., PERL),

c. the Mozilla Public License,

d. the Netscape Public License,

e. the Sun Community Source License (SCSL),

f. vi) the Sun Industry Source License (SISL),

g. vii) the Apache Software license, and

h. 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.

Configuring Request Logging

Overview: Configuring a Request Logging profile

The Request Logging profile gives you the ability to configure data within a log file for HTTP requests and responses, in accordance with specified parameters.

Task summary

Perform these tasks to log HTTP request and response data.

Creating a pool with request logging to manage HTTP traffic
Creating a request logging profile
Configuring a virtual server for request logging
Deleting a request logging profile

Creating a pool with request logging to manage HTTP traffic

For a basic configuration, you need to create a pool to manage HTTP connections.

1. On the Main tab, click **Local Traffic** > **Pools**.
   The Pool List screen opens.
2. Click **Create**.
   The New Pool screen opens.
3. In the **Name** field, type a unique name for the pool.
4. For the **Health Monitors** setting, from the **Available** list, select the **http** monitor and move the monitor to the **Active** list.
5. From the **Load Balancing Method** list, select how the system distributes traffic to members of this pool.

   The default is **Round Robin**.
6. For the **Priority Group Activation** setting, specify how to handle priority groups:
   - Select **Disabled** to disable priority groups. This is the default option.
   - Select **Less than**, and in the **Available Members** field type the minimum number of members that must remain available in each priority group in order for traffic to remain confined to that group.
7. Add the IP address for each logging server that you want to include in the pool, using the **New Members** setting:
   a) Type an IP address in the **Address**, field or select a node address from the **Node List**.
   b) Type the port number for the logging server in the **Service Port** field.
   c) (Optional) Type a priority number in the **Priority** field.
   d) Click **Add**.
8. Click **Finished**.

The new pool appears in the Pools list.

Creating a request logging profile

You must have already created a pool that includes logging servers as pool members before you can create a request logging profile.

With a request logging profile, you can log specified data for HTTP requests and responses, and then use that information for analysis and troubleshooting.

1. On the Main tab, click **Local Traffic** > **Profiles** > **Other** > **Request Logging**.
   The Request Logging profile list screen opens.
2. Click **Create**.
   The New Request Logging Profile screen opens.
3. From the **Parent Profile** list, select a profile from which the new profile inherits properties.
4. Select the **Custom** check box for the Request Settings area.
5. Configure the request settings, as necessary.
6. Select the **Custom** check box for the Response Settings area.
7. Configure the response settings, as necessary.
8. Click **Finished**.

This makes a request logging profile available to log specified data for HTTP requests and responses.

You must configure a virtual server for request logging.

Configuring a request logging profile for requests

Ensure that the configuration includes a pool that includes logging servers as pool members.

You can use a request logging profile to log specified data for HTTP requests, and then use that information for analysis and troubleshooting.

1. On the Main tab, click **Local Traffic** > **Profiles** > **Other** > **Request Logging**.
   The Request Logging profile list screen opens.
2. Click **Create**.
   The New Request Logging Profile screen opens.
3. From the **Parent Profile** list, select a profile from which the new profile inherits properties.
4. Select the **Custom** check box for the Request Settings area.
5. From the **Request Logging** list, select **Enabled**.
6. In the **Template** field, type the request logging parameters for the entries that you want to include in the log file.
7. From the **HSL Protocol** list, select a high-speed logging protocol.
8. From the **Pool Name** list, select the pool that includes the log server as a pool member.
9. (Optional) You can also configure the error response settings.
   a) From the **Respond On Error** list, select **Enabled**.
   b) In the **Error Response** field, type the error response strings that you want to include in the log file. These strings must be well-formed for the protocol serving the strings.
   c) Select the **Close On Error** check box to drop the request and close the connection if logging fails.
10. (Optional) You can also configure the logging request errors settings.
    a) From the **Log Logging Errors** list, select **Enabled**.

b) In the **Error Template** field, type the request logging parameters for the entries that you want to include in the log file.
c) From the **HSL Error Protocol** list, select a high-speed logging error protocol.
d) From the **Error Pool Name** list, select a pool that includes the node for the error logging server as a pool member.

11. Click **Update**.

This configures a request logging profile to log specified data for HTTP requests.

Configuring a request logging profile for responses

You must have already created a pool that includes logging servers as pool members before you can configure a request logging profile for responses.

With a request logging profile, you can log specified data for HTTP requests and responses, and then use that information for analysis and troubleshooting.

1. On the Main tab, click **Local Traffic** > **Profiles** > **Other** > **Request Logging**.
The Request Logging profile list screen opens.
2. From the **Parent Profile** list, select a profile from which the new profile inherits properties.
3. Select the **Custom** check box for the Response Settings area.
4. In the Response Settings area, from the **Response Logging** list, select **Enabled**.
5. (Optional) Select the **Log By Default** check box.
The **Log By Default** check box is selected by default.
6. In the **Template** field, type the response logging parameters for the entries that you want to include in the log file.
7. From the **HSL Protocol** list, select a high-speed logging protocol.
8. From the **Pool Name** list, select the pool that includes the node log server as a pool member.
9. (Optional) Configure the logging request error settings.
a) From the **Log Logging Errors** list, select **Enabled**.
b) In the **Error Template** field, type the response logging parameters for the entries that you want to include in the log file.
c) From the **HSL Error Protocol** list, select a high-speed logging error protocol.
d) From the **Error Pool Name** list, select a pool that includes the node for the error log server as a pool member.

10. Click **Update** to save the changes.

This configures a request logging profile to log specified data for HTTP responses.

Configuring a virtual server for request logging

You can configure a virtual server to pass traffic to logging servers.

1. On the Main tab, click **Local Traffic** > **Virtual Servers**.
The Virtual Server List screen opens.
2. Click the name of the virtual server you want to modify.
3. On the menu bar, click **Resources**.

4. From the **Default Pool** list, select a pool name that is configured with pool members for request logging.
5. Click the **Properties** tab.
6. From the **Configuration** list, select **Advanced**.
7. From the **Request Logging Profile** list, select the profile you want to assign to the virtual server.
8. Click **Update**.

This virtual server can now pass traffic to the configured logging servers.

Deleting a request logging profile

You can delete a user-defined request logging profile that is obsolete or no longer needed.

1. On the Main tab, click **Local Traffic** > **Profiles** > **Other** > **Request Logging**.
   The Request Logging profile list screen opens.
2. Select the check box for the applicable profile.
3. Click **Delete**.
4. Click **Delete**.

The profile is deleted.

Request Logging profile settings

With the Request Logging profile, you can specify the data and the format for HTTP requests and responses that you want to include in a log file.

General Properties

Setting	Value	Description
Name	No default	Specifies the name of the profile.
Parent Profile	Selected predefined or user-defined profile	Specifies the selected predefined or user-defined profile.

Request Settings

Setting	Value	Description
Request Logging	Disabled	Enables logging for requests.
Template		Specifies the directives and entries to be logged.
HSL Protocol	UDP	Specifies the protocol to be used for high-speed logging of requests.
Pool Name	None	Defines the pool associated with the virtual server that is logged.
Respond On Error	Disabled	Enables the ability to respond when an error occurs.

Setting	Value	Description
Error Response	None	Specifies the response text to be used when an error occurs. For example, the following response text provides content for a 503 error. `<html> <head> <title>ERROR</title> </head> <body> <p>503 ERROR-Service Unavailable</p> </body> </html>`
Close On Error	Disabled	When enabled, and logging fails, drops the request and closes the connection.
Log Logging Errors	Disabled	Enables the ability to log any errors when logging requests.
Error Template	None	Defines the format for requests in an error log.
HSL Error Protocol	UDP	Defines the protocol to be used for high-speed logging of request errors.
Error Pool Name	None	Specifies the name of the error logging pool for requests.

Response Settings

Setting	Value	Description
Response Logging	Disabled	Enables logging for responses.
Log By Default	Enabled	Defines whether to log the specified settings for responses by default.
Template	None	Specifies the directives and entries to be logged.
HSL Protocol	UDP	Specifies the protocol to be used for high-speed logging of responses.
Pool Name	None	Defines the pool name associated with the virtual server that is logged.
Log Logging Errors	Disabled	Enables the ability to log any errors when logging responses.
Error Template	None	Defines the format for responses in an error log.
HSL Error Protocol	UDP	Defines the protocol to be used for high-speed logging of response errors.
Error Pool Name	None	Specifies the name of the error logging pool for responses.

Request Logging parameters

This table lists all available parameters from which you can create a custom HTTP Request Logging profile. These are used to specify entries for the **Template** and **Error Template** settings For each parameter, the system writes to the log the information described in the right column.

Table 1: Request logging parameters

Parameter	Log file entry description
BIGIP_BLADE_ID	An entry for the slot number of the blade that handled the request.
BIGIP_CACHED	An entry of `Cached status: true`, if the response came from BIG-IP® cache, or `Cached status: false`, if the response came from the server.
BIGIP_HOSTNAME	An entry for the configured host name of the unit or chassis.
CLIENT_IP	An entry for the IP address of a client, for example, `192.168.74.164`.
CLIENT_PORT	An entry for the port of a client, for example, `80`.
DATE_D	A two-character entry for the day of the month, ranging from ` 1` (note the leading space) through `31`.
DATE_DAY	An entry that spells out the name of the day.
DATE_DD	A two-digit entry for the day of the month, ranging from `01` through `31`.
DATE_DY	A three-letter entry for the day, for example, `Mon`.
DATE_HTTP	A date and time entry in an HTTP format, for example, `Tue, 5 Apr 2011 02:15:31 GMT`.
DATE_MM	A two-digit month entry, ranging from `01` through `12`.
DATE_MON	A three-letter abbreviation for a month entry, for example, `APR`.
DATE_MONTH	An entry that spells out the name of the month.
DATE_NCSA	A date and time entry in an NCSA format, for example, `dd/mm/yy:hh:mm:ss ZNE`.
DATE_YY	A two-digit year entry, ranging from `00` through `99`.
DATE_YYYY	A four-digit year entry.
HTTP_CLASS	The name of the `httpclass` profile that matched the request, or an empty entry if a profile name is not associated with the request.
HTTP_KEEPALIVE	A flag summarizing the HTTP1.1 `keep-alive` status for the request:: a`Y` if the HTTP1.1 `keep-alive` header was sent, or an empty entry if not.
HTTP_METHOD	An entry that defines the HTTP method, for example, `GET`, `PUT`, `HEAD`, `POST`, `DELETE`, `TRACE`, or `CONNECT`.
HTTP_PATH	An entry that defines the HTTP path.
HTTP_QUERY	The text following the first `?` in the URI.
HTTP_REQUEST	The complete text of the request, for example, `$METHOD $URI $VERSION`.
HTTP_STATCODE	The numerical response status code, that is, the status response code excluding subsequent text.
HTTP_STATUS	The complete status response, that is, the number appended with any subsequent text.

Parameter	Log file entry description
HTTP_URI	An entry for the URI of the request.
HTTP_VERSION	An entry that defines the HTTP version.
NCSA_COMBINED	An NCSA Combined formatted log string, for example, `$NCSA_COMMON $Referer ${User-agent} $Cookie`.
NCSA_COMMON	An NCSA Common formatted log string, for example, `$CLIENT_IP - - $DATE_NCSA $HTTP_REQUEST $HTTP_STATCODE $RESPONSE_SIZE`.
RESPONSE_MSECS	The elapsed time in milliseconds (ms) between receiving the request and sending the response.
RESPONSE_SIZE	An entry for the size of response in bytes.
RESPONSE_USECS	The elapsed time in microseconds (µs) between receiving the request and sending the response.
SERVER_IP	An entry for the IP address of a server, for example, `10.10.0.1`.
SERVER_PORT	An entry for the port of a logging server.
SNAT_IP	An entry for the self IP address of the BIG-IP-originated connection to the server when SNAT is enabled, or an entry for the client IP address when SNAT is not enabled.
SNAT_PORT	An entry for the port of the BIG-IP-originated connection to the server when SNAT is enabled, or an entry for the client port when SNAT is not enabled.
TIME_AMPM	A twelve-hour request-time qualifier, for example, `AM` or `PM`.
TIME_H12	A compact twelve-hour time entry for request-time hours, ranging from `1` through `12`.
TIME_HRS	A twelve-hour time entry for hours, for example, `12 AM`.
TIME_HH12	A twelve hour entry for request-time hours, ranging from `01` through `12`.
TIME_HMS	An entry for a compact request time of `H:M:S`, for example, `12:10:49`.
TIME_HH24	A twenty-four hour entry for request-time hours, ranging from `00` through `23`.
TIME_MM	A two-digit entry for minutes, ranging from `00` through `59`.
TIME_MSECS	An entry for the request-time fraction in milliseconds (ms).
TIME_OFFSET	An entry for the time zone, offset in hours from GMT, for example, `-11`.
TIME_SS	A two-digit entry for seconds, ranging from `00` through `59`.
TIME_UNIX	A UNIX time entry for the number of seconds since the UNIX epoch, for example, `00:00:00 UTC, January 1st, 1970`.
TIME_USECS	An entry for the request-time fraction in microseconds (µs).
TIME_ZONE	An entry for the current Olson database or tz database three-character time zone, for example, `PDT`.
VIRTUAL_IP	An entry for the IP address of a virtual server, for example, `192.168.10.1`.
VIRTUAL_NAME	An entry for the name of a virtual server.
VIRTUAL_POOL_NAME	An entry for the name of the pool containing the responding server.
VIRTUAL_PORT	An entry for the port of a virtual server, for example, `80`.

Parameter	Log file entry description
VIRTUAL_SNATPOOL_NAME	The name of the Secure Network Address Translation pool associated with the virtual server.
NULL	Undelineated strings return the value of the respective header.

Configuring Remote High-Speed Logging of BIG-IP System Processes

Overview: Configuring high-speed remote logging of BIG-IP system processes

You can configure the BIG-IP® system to log information about BIG-IP system processes and send the log messages to remote high-speed log servers. You can filter the data that the system logs based on alert-level and source.

When configuring remote high-speed logging of BIG-IP system processes, it is helpful to understand the objects you need to create and why, as described here:

Object	Reason
Pool of remote log servers	Create a pool of remote log servers to which the BIG-IP system can send log messages.
Destination (unformatted)	Create a log destination of Remote High-Speed Log type that specifies a pool of remote log servers.
Destination (formatted)	If your remote log servers are the ArcSight, Splunk, IPFIX, or Remote Syslog type, create an additional log destination to format the logs in the required format and forward the logs to a remote high-speed log destination.
Publisher	Create a log publisher to send logs to a set of specified log destinations.
Filter	Create a log filter to define the messages to be included in the BIG-IP system logs and associate a log publisher with the filter.

This illustration shows the association of the configuration objects for remote high-speed logging of BIG-IP system processes.

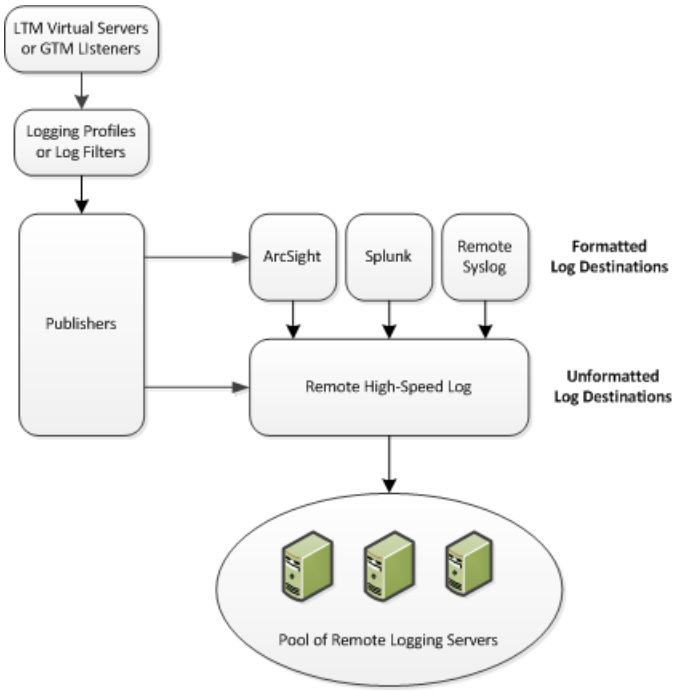

Figure 1: Association of remote high-speed logging configuration objects

Task summary

Perform these tasks to configure BIG-IP® system logging.

Note: *Enabling remote high-speed logging impacts BIG-IP system performance.*

Creating a pool of remote logging servers
Creating a remote high-speed log destination
Creating a formatted remote high-speed log destination
Creating a publisher
Creating a logging filter
Disabling system logging
Troubleshooting logs that contain unexpected messages

Creating a pool of remote logging servers

Before creating a pool of log servers, gather the IP addresses of the servers that you want to include in the pool. Ensure that the remote log servers are configured to listen to and receive log messages from the BIG-IP® system.

Create a pool of remote log servers to which the BIG-IP system can send log messages.

1. On the Main tab, click the applicable path.
   - **DNS** > **Delivery** > **Load Balancing** > **Pools**
   - **Local Traffic** > **Pools**

   The Pool List screen opens.
2. Click **Create**.
   The New Pool screen opens.

3. In the **Name** field, type a unique name for the pool.
4. Using the **New Members** setting, add the IP address for each remote logging server that you want to include in the pool:
   a) Type an IP address in the **Address** field, or select a node address from the **Node List**.
   b) Type a service number in the **Service Port** field, or select a service name from the list.

   Note: *Typical remote logging servers require port* `514`*.*

   c) Click **Add**.
5. Click **Finished**.

Creating a remote high-speed log destination

Before creating a remote high-speed log destination, ensure that at least one pool of remote log servers exists on the BIG-IP® system.

Create a log destination of the **Remote High-Speed Log** type to specify that log messages are sent to a pool of remote log servers.

1. On the Main tab, click **System** > **Logs** > **Configuration** > **Log Destinations**.
   The Log Destinations screen opens.
2. Click **Create**.
3. In the **Name** field, type a unique, identifiable name for this destination.
4. From the **Type** list, select **Remote High-Speed Log**.

   Important: *If you use log servers such as Remote Syslog, Splunk, or ArcSight, which require data be sent to the servers in a specific format, you must create an additional log destination of the required type, and associate it with a log destination of the* ***Remote High-Speed Log*** *type. With this configuration, the BIG-IP system can send data to the servers in the required format.*

   The BIG-IP system is configured to send an unformatted string of text to the log servers.
5. From the **Pool Name** list, select the pool of remote log servers to which you want the BIG-IP system to send log messages.
6. From the **Protocol** list, select the protocol used by the high-speed logging pool members.
7. Click **Finished**.

Creating a formatted remote high-speed log destination

Ensure that at least one remote high-speed log destination exists on the BIG-IP® system.

Create a formatted logging destination to specify that log messages are sent to a pool of remote log servers, such as Remote Syslog, Splunk, or ArcSight servers.

1. On the Main tab, click **System** > **Logs** > **Configuration** > **Log Destinations**.
   The Log Destinations screen opens.
2. Click **Create**.
3. In the **Name** field, type a unique, identifiable name for this destination.

4. From the **Type** list, select a formatted logging destination, such as **IPFIX**, **Remote Syslog**, **Splunk**, or **ArcSight**.

   Important: *ArcSight formatting is only available for logs coming from Advanced Firewall Manager (AFM), Application Security Manager™ (ASM), and the Secure Web Gateway component of Access Policy Manager® (APM®). IPFIX is not available for Secure Web Gateway. Remote Syslog formatting is the only type supported for logs coming from APM. The Splunk format is a predefined format of key value pairs.*

   The BIG-IP system is configured to send a formatted string of text to the log servers.
5. If you selected **Remote Syslog**, from the **Syslog Format** list, select a format for the logs, and then from the **High-Speed Log Destination** list, select the destination that points to a pool of remote Syslog servers to which you want the BIG-IP system to send log messages.

   Important: *For logs coming from Access Policy Manager® (APM®), only the BSD Syslog format is supported.*

6. If you selected **Splunk** or **IPFIX**, from the **Forward To** list, select the destination that points to a pool of high-speed log servers to which you want the BIG-IP system to send log messages.
7. Click **Finished**.

Creating a publisher

Ensure that at least one destination associated with a pool of remote log servers exists on the BIG-IP® system.

Create a publisher to specify where the BIG-IP system sends log messages for specific resources.

1. On the Main tab, click **System** > **Logs** > **Configuration** > **Log Publishers**.
   The Log Publishers screen opens.
2. Click **Create**.
3. In the **Name** field, type a unique, identifiable name for this publisher.
4. For the **Destinations** setting, select a destination from the **Available** list, and click **<<** to move the destination to the **Selected** list.

   Note: *If you are using a formatted destination, select the destination that matches your log servers, such as Remote Syslog, Splunk, or ArcSight.*

5. Click **Finished**.

Creating a logging filter

Ensure that at least one log publisher is configured on the BIG-IP® system.

Create a custom log filter to specify the system log messages that you want to publish to a particular log.

1. On the Main tab, click **System** > **Logs** > **Configuration** > **Log Filters**.
   The Log Filters screen opens.
2. In the **Name** field, type a unique, identifiable name for this filter.
3. From the **Severity** list, select the level of alerts that you want the system to use for this filter.

Note: *The severity level that you select includes all of the severity levels that display above your selection in the list. For example, if you select* ***Emergency****, the system publishes only emergency messages to the log. If you select* ***Critical****, the system publishes critical, alert, and emergency-level messages in the log.*

4. From the **Source** list, select the system processes from which messages will be sent to the log.
5. In the **Message ID** field, type the first eight hex-digits of the specific message ID that you want the system to include in the log. Use this field when you want a log to contain only each instance of one specific log message.

Note: *BIG-IP system log messages contain message ID strings in the format:* `xxxxxxxx:x:`*. For example, in this log message:* `Oct 31 11:06:27 olgavmmgmt notice mcpd[5641]: 01070410:5: Removed subscription with subscriber id lind` *, the message ID string is:* `01070410:5:`*. You enter only the first eight hex-digits:* `01070410`*.*

6. From the **Log Publisher** list, select the publisher that includes the destinations to which you want to send log messages.
7. Click **Finished**.

Disabling system logging

When you no longer want the BIG-IP® system to log information about its internal systems, you can delete the log filter that you created. For example, when mitigating a DoS attack, if you created a log filter that includes only one specific message in the log, you can delete that log filter once you handle the attack.

1. On the Main tab, click **System** > **Logs** > **Configuration** > **Log Filters**.
   The Log Filters screen opens.
2. Select the check box next to the name of the log filter that you want to delete. Click **Delete**, and then click **Delete** again.

Troubleshooting logs that contain unexpected messages

If you configured a filter to send all instances of a specific message ID to your remote logging servers and this message ID is still displaying in the local log in the BIG-IP system, you can disable legacy log message processing in order to display instances of this message ID only on the remote logging servers.

Important: *When you create a filter that disables legacy log message processing, the legacy logs are completely disabled. Therefore, you must also create a filter for every source from which you want log messages to be sent to the pool of remote log servers.*

1. On the Main tab, click **System** > **Logs** > **Configuration** > **Log Filters**.
   The Log Filters screen opens.
2. Click **Create**.
3. In the **Name** field, type a unique, identifiable name for this filter.
4. From the **Severity** list, select **Debug**.
5. From the **Source** list, select **All**.
6. From the **Log Publisher** list, select **None**.
7. Click **Finished**.

Configuring Remote High-Speed DNS Logging

Overview: Configuring remote high-speed DNS logging

You can configure the BIG-IP® system to log information about DNS traffic and send the log messages to remote high-speed log servers. You can choose to log either DNS queries or DNS responses, or both. In addition, you can configure the system to perform logging on DNS traffic differently for specific resources. For example, you can configure logging for a specific resource, and then disable and re-enable logging for the resource based on your network administration needs.

When configuring remote high-speed DNS logging, it is helpful to understand the objects you need to create and why, as described here:

Object	Reason
Pool of remote log servers	Create a pool of remote log servers to which the BIG-IP system can send log messages.
Destination (unformatted)	Create a log destination of Remote High-Speed Log type that specifies a pool of remote log servers.
Destination (formatted)	If your remote log servers are the ArcSight, Splunk, IPFIX, or Remote Syslog type, create an additional log destination to format the logs in the required format and forward the logs to a remote high-speed log destination.
Publisher	Create a log publisher to send logs to a set of specified log destinations.
DNS Logging profile	Create a custom DNS Logging profile to define the data you want the BIG-IP system to include in the DNS logs and associate a log publisher with the profile.
DNS profile	Create a custom DNS profile to enable DNS logging, and associate a DNS Logging profile with the DNS profile.
LTM® virtual server	Associate a custom DNS profile with a virtual server to define how the BIG-IP system logs the DNS traffic that the virtual server processes.
GTM™ listener	Associate a custom DNS profile with a listener to define how the BIG-IP system logs the DNS traffic that the listener processes.

This illustration shows the association of the configuration objects for remote high-speed logging.

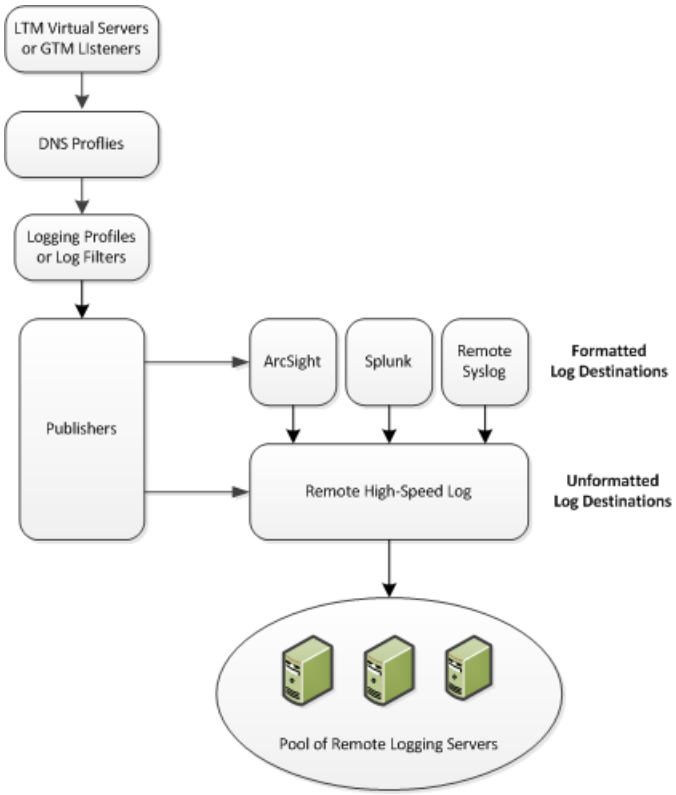

Figure 2: Association of remote high-speed logging configuration objects

Task summary

Creating a pool of remote logging servers
Creating a remote high-speed log destination
Creating a formatted remote high-speed log destination
Creating a publisher
Creating a custom DNS logging profile for logging DNS queries
Creating a custom DNS logging profile for logging DNS responses
Creating a custom DNS logging profile for logging DNS queries and responses
Creating a custom DNS profile to enable DNS logging
Configuring a listener for DNS logging
Configuring an LTM virtual server for DNS logging
Disabling DNS logging

Creating a pool of remote logging servers

Before creating a pool of log servers, gather the IP addresses of the servers that you want to include in the pool. Ensure that the remote log servers are configured to listen to and receive log messages from the BIG-IP® system.

Create a pool of remote log servers to which the BIG-IP system can send log messages.

1. On the Main tab, click the applicable path.
   - **DNS** > **Delivery** > **Load Balancing** > **Pools**
   - **Local Traffic** > **Pools**

The Pool List screen opens.

2. Click **Create**.
   The New Pool screen opens.
3. In the **Name** field, type a unique name for the pool.
4. Using the **New Members** setting, add the IP address for each remote logging server that you want to include in the pool:
   a) Type an IP address in the **Address** field, or select a node address from the **Node List**.
   b) Type a service number in the **Service Port** field, or select a service name from the list.

   Note: *Typical remote logging servers require port* `514`*.*

   c) Click **Add**.
5. Click **Finished**.

Creating a remote high-speed log destination

Before creating a remote high-speed log destination, ensure that at least one pool of remote log servers exists on the BIG-IP® system.

Create a log destination of the **Remote High-Speed Log** type to specify that log messages are sent to a pool of remote log servers.

1. On the Main tab, click **System** > **Logs** > **Configuration** > **Log Destinations**.
   The Log Destinations screen opens.
2. Click **Create**.
3. In the **Name** field, type a unique, identifiable name for this destination.
4. From the **Type** list, select **Remote High-Speed Log**.

   Important: *If you use log servers such as Remote Syslog, Splunk, or ArcSight, which require data be sent to the servers in a specific format, you must create an additional log destination of the required type, and associate it with a log destination of the* ***Remote High-Speed Log*** *type. With this configuration, the BIG-IP system can send data to the servers in the required format.*

   The BIG-IP system is configured to send an unformatted string of text to the log servers.
5. From the **Pool Name** list, select the pool of remote log servers to which you want the BIG-IP system to send log messages.
6. From the **Protocol** list, select the protocol used by the high-speed logging pool members.
7. Click **Finished**.

Creating a formatted remote high-speed log destination

Ensure that at least one remote high-speed log destination exists on the BIG-IP® system.

Create a formatted logging destination to specify that log messages are sent to a pool of remote log servers, such as Remote Syslog, Splunk, or ArcSight servers.

1. On the Main tab, click **System** > **Logs** > **Configuration** > **Log Destinations**.
   The Log Destinations screen opens.

2. Click **Create**.
3. In the **Name** field, type a unique, identifiable name for this destination.
4. From the **Type** list, select a formatted logging destination, such as **IPFIX**, **Remote Syslog**, **Splunk**, or **ArcSight**.

   Important: *ArcSight formatting is only available for logs coming from Advanced Firewall Manager (AFM), Application Security Manager™ (ASM), and the Secure Web Gateway component of Access Policy Manager® (APM®). IPFIX is not available for Secure Web Gateway. Remote Syslog formatting is the only type supported for logs coming from APM. The Splunk format is a predefined format of key value pairs.*

   The BIG-IP system is configured to send a formatted string of text to the log servers.
5. If you selected **Remote Syslog**, from the **Syslog Format** list, select a format for the logs, and then from the **High-Speed Log Destination** list, select the destination that points to a pool of remote Syslog servers to which you want the BIG-IP system to send log messages.

   Important: *For logs coming from Access Policy Manager® (APM®), only the BSD Syslog format is supported.*

6. If you selected **Splunk** or **IPFIX**, from the **Forward To** list, select the destination that points to a pool of high-speed log servers to which you want the BIG-IP system to send log messages.
7. Click **Finished**.

Creating a publisher

Ensure that at least one destination associated with a pool of remote log servers exists on the BIG-IP® system.

Create a publisher to specify where the BIG-IP system sends log messages for specific resources.

1. On the Main tab, click **System** > **Logs** > **Configuration** > **Log Publishers**.
   The Log Publishers screen opens.
2. Click **Create**.
3. In the **Name** field, type a unique, identifiable name for this publisher.
4. For the **Destinations** setting, select a destination from the **Available** list, and click **<<** to move the destination to the **Selected** list.

   Note: *If you are using a formatted destination, select the destination that matches your log servers, such as Remote Syslog, Splunk, or ArcSight.*

5. Click **Finished**.

Creating a custom DNS logging profile for logging DNS queries

Create a custom DNS logging profile to log DNS queries, when you want to log only DNS queries.

1. On the Main tab, click **DNS** > **Delivery** > **Profiles** > **Other** > **DNS Logging** or **Local Traffic** > **Profiles** > **Other** > **DNS Logging**.
   The DNS Logging profile list screen opens.
2. Click **Create**.

The New DNS Logging profile screen opens.

3. In the **Name** field, type a unique name for the profile.
4. From the **Log Publisher** list, select a destination to which the BIG-IP system sends DNS log entries.
5. For the **Log Queries** setting, ensure that the **Enabled** check box is selected, if you want the BIG-IP system to log all DNS queries.
6. For the **Include Query ID** setting, select the **Enabled** check box, if you want the BIG-IP system to include the query ID sent by the client in the log messages.
7. Click **Finished**.

Assign this custom DNS logging profile to a custom DNS profile.

Creating a custom DNS logging profile for logging DNS responses

Create a custom DNS logging profile to log DNS responses when you want to determine how the BIG-IP system is responding to a given query.

1. On the Main tab, click **DNS** > **Delivery** > **Profiles** > **Other** > **DNS Logging** or **Local Traffic** > **Profiles** > **Other** > **DNS Logging**.
   The DNS Logging profile list screen opens.
2. Click **Create**.
   The New DNS Logging profile screen opens.
3. In the **Name** field, type a unique name for the profile.
4. From the **Log Publisher** list, select a destination to which the BIG-IP system sends DNS log entries.
5. For the **Log Responses** setting, select the **Enabled** check box, if you want the BIG-IP system to log all DNS responses.
6. For the **Include Query ID** setting, select the **Enabled** check box, if you want the BIG-IP system to include the query ID sent by the client in the log messages.
7. Click **Finished**.

Assign this custom DNS logging profile to a custom DNS profile.

Creating a custom DNS logging profile for logging DNS queries and responses

Create a custom DNS logging profile to log both DNS queries and responses when troubleshooting a DDoS attack.

Note: *Logging both DNS queries and responses has an impact on the BIG-IP® system performance.*

---

1. On the Main tab, click **DNS** > **Delivery** > **Profiles** > **Other** > **DNS Logging** or **Local Traffic** > **Profiles** > **Other** > **DNS Logging**.
   The DNS Logging profile list screen opens.
2. Click **Create**.
   The New DNS Logging profile screen opens.
3. In the **Name** field, type a unique name for the profile.
4. From the **Log Publisher** list, select a destination to which the BIG-IP system sends DNS log entries.
5. For the **Log Queries** setting, ensure that the **Enabled** check box is selected, if you want the BIG-IP system to log all DNS queries.

6. For the **Log Responses** setting, select the **Enabled** check box, if you want the BIG-IP system to log all DNS responses.
7. For the **Include Query ID** setting, select the **Enabled** check box, if you want the BIG-IP system to include the query ID sent by the client in the log messages.
8. Click **Finished**.

Assign this custom DNS logging profile to a custom DNS profile.

Creating a custom DNS profile to enable DNS logging

Ensure that at least one custom DNS Logging profile exists on the BIG-IP® system.

Create a custom DNS profile to log specific information about DNS traffic processed by the resources to which the DNS profile is assigned. Depending upon what information you want the BIG-IP system to log, attach a custom DNS Logging profile configured to log DNS queries, to log DNS responses, or to log both.

1. On the Main tab, click **DNS** > **Delivery** > **Profiles** > **DNS** or **Local Traffic** > **Profiles** > **Services** > **DNS**.
   The DNS profile list screen opens.
2. Click **Create**.
   The New DNS Profile screen opens.
3. In the **Name** field, type a unique name for the profile.
4. Select the **Custom** check box.
5. In the Logging and Reporting area, from the **Logging** list, select **Enabled**.
6. In the Logging and Reporting area, from the **Logging Profile** list, select a custom DNS Logging profile.
7. Click **Finished**.

You must assign this custom DNS profile to a resource before the BIG-IP system can log information about the DNS traffic handled by the resource.

Configuring a listener for DNS logging

Ensure that at least one custom DNS profile with logging configured exists on the BIG-IP® system.

Assign a custom DNS profile to a listener when you want the BIG-IP system to log the DNS traffic the listener handles.

Note: *This task applies only to GTM™-provisioned systems.*

---

1. On the Main tab, click **DNS** > **Delivery** > **Listeners**.
   The Listeners List screen opens.
2. Click the name of the listener you want to modify.
3. In the Service area, from the **DNS Profile** list, select a custom DNS profile that is associated with a DNS Logging profile.
4. Click **Update**.

Configuring an LTM virtual server for DNS logging

Ensure that at least one custom DNS profile with logging enabled exists on the BIG-IP® system.

Assign a custom DNS profile with logging enabled to a virtual server when you want the BIG-IP system to log the DNS traffic the virtual server handles.

Note: *This task applies only to LTM®-provisioned systems.*

1. On the Main tab, click **Local Traffic** > **Virtual Servers**.
   The Virtual Server List screen opens.
2. Click the name of the virtual server you want to modify.
3. From the **Configuration** list, select **Advanced**.
4. From the **DNS Profile** list, select a custom DNS profile that is associated with a DNS Logging profile.
5. Click **Update** to save the changes.

Disabling DNS logging

Disable DNS logging on a custom DNS profile when you no longer want the BIG-IP® system to log information about the DNS traffic handled by the resources to which the profile is assigned.

Note: *You can disable and re-enable DNS logging for a specific resource based on your network administration needs.*

1. On the Main tab, click **DNS** > **Delivery** > **Profiles** > **DNS**.
   The DNS profile list screen opens.
2. Click the name of a profile.
3. Select the **Custom** check box.
4. In the Logging and Reporting area, from the **Logging** list, select **Disabled**.
5. Click **Update**.

The BIG-IP system does not perform DNS logging on the DNS traffic handled by the resources to which this profile is assigned.

Implementation result

You now have an implementation in which the BIG-IP® system performs DNS logging on specific DNS traffic and sends the log messages to a pool of remote log servers.

Configuring Remote High-Speed Logging of Protocol Security Events

Overview: Configuring Remote Protocol Security Event Logging

You can configure the BIG-IP® system to log information about BIG-IP system Protocol Security events and send the log messages to remote high-speed log servers.

Important: *The Advanced Firewall Manager™ (AFM™) must be licensed and provisioned before you can configure Protocol Security event logging.*

When configuring remote high-speed logging of Protocol Security events, it is helpful to understand the objects you need to create and why, as described here:

Object	Reason
Pool of remote log servers	Create a pool of remote log servers to which the BIG-IP system can send log messages.
Destination (unformatted)	Create a log destination of Remote High-Speed Log type that specifies a pool of remote log servers.
Destination (formatted)	If your remote log servers are the ArcSight, Splunk, IPFIX, or Remote Syslog type, create an additional log destination to format the logs in the required format and forward the logs to a remote high-speed log destination.
Publisher	Create a log publisher to send logs to a set of specified log destinations.
Logging profile	Create a custom Logging profile to enable logging of user-specified data at a user-specified level, and associate a log publisher with the profile.
LTM® virtual server	Associate a custom Logging profile with a virtual server to define how the BIG-IP system logs security events on the traffic that the virtual server processes.

This illustration shows the association of the configuration objects for remote high-speed logging.

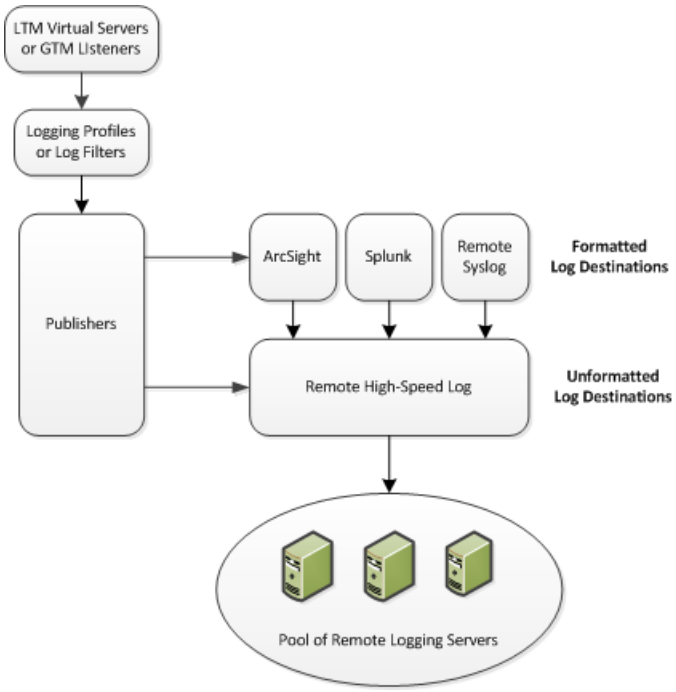

Figure 3: Association of remote high-speed logging configuration objects

Task summary

Perform these tasks to configure Protocol Security event logging on the BIG-IP® system.

Note: *Enabling remote high-speed logging impacts BIG-IP system performance.*

Creating a pool of remote logging servers
Creating a remote high-speed log destination
Creating a formatted remote high-speed log destination
Creating a publisher
Creating a custom Protocol Security Logging profile
Configuring a virtual server for Protocol Security event logging
Disabling logging

Creating a pool of remote logging servers

Before creating a pool of log servers, gather the IP addresses of the servers that you want to include in the pool. Ensure that the remote log servers are configured to listen to and receive log messages from the BIG-IP® system.

Create a pool of remote log servers to which the BIG-IP system can send log messages.

1. On the Main tab, click the applicable path.
   - **DNS** > **Delivery** > **Load Balancing** > **Pools**
   - **Local Traffic** > **Pools**

   The Pool List screen opens.
2. Click **Create**.
   The New Pool screen opens.

3. In the **Name** field, type a unique name for the pool.
4. Using the **New Members** setting, add the IP address for each remote logging server that you want to include in the pool:
   a) Type an IP address in the **Address** field, or select a node address from the **Node List**.
   b) Type a service number in the **Service Port** field, or select a service name from the list.

   Note: *Typical remote logging servers require port* `514`*.*

   c) Click **Add**.
5. Click **Finished**.

Creating a remote high-speed log destination

Before creating a remote high-speed log destination, ensure that at least one pool of remote log servers exists on the BIG-IP® system.

Create a log destination of the **Remote High-Speed Log** type to specify that log messages are sent to a pool of remote log servers.

1. On the Main tab, click **System** > **Logs** > **Configuration** > **Log Destinations**.
   The Log Destinations screen opens.
2. Click **Create**.
3. In the **Name** field, type a unique, identifiable name for this destination.
4. From the **Type** list, select **Remote High-Speed Log**.

   Important: *If you use log servers such as Remote Syslog, Splunk, or ArcSight, which require data be sent to the servers in a specific format, you must create an additional log destination of the required type, and associate it with a log destination of the* ***Remote High-Speed Log*** *type. With this configuration, the BIG-IP system can send data to the servers in the required format.*

   The BIG-IP system is configured to send an unformatted string of text to the log servers.
5. From the **Pool Name** list, select the pool of remote log servers to which you want the BIG-IP system to send log messages.
6. From the **Protocol** list, select the protocol used by the high-speed logging pool members.
7. Click **Finished**.

Creating a formatted remote high-speed log destination

Ensure that at least one remote high-speed log destination exists on the BIG-IP® system.

Create a formatted logging destination to specify that log messages are sent to a pool of remote log servers, such as Remote Syslog, Splunk, or ArcSight servers.

1. On the Main tab, click **System** > **Logs** > **Configuration** > **Log Destinations**.
   The Log Destinations screen opens.
2. Click **Create**.
3. In the **Name** field, type a unique, identifiable name for this destination.

4. From the **Type** list, select a formatted logging destination, such as **IPFIX**, **Remote Syslog**, **Splunk**, or **ArcSight**.

   Important: *ArcSight formatting is only available for logs coming from Advanced Firewall Manager (AFM), Application Security Manager™ (ASM), and the Secure Web Gateway component of Access Policy Manager® (APM®). IPFIX is not available for Secure Web Gateway. Remote Syslog formatting is the only type supported for logs coming from APM. The Splunk format is a predefined format of key value pairs.*

   The BIG-IP system is configured to send a formatted string of text to the log servers.
5. If you selected **Remote Syslog**, from the **Syslog Format** list, select a format for the logs, and then from the **High-Speed Log Destination** list, select the destination that points to a pool of remote Syslog servers to which you want the BIG-IP system to send log messages.

   Important: *For logs coming from Access Policy Manager® (APM®), only the BSD Syslog format is supported.*

6. If you selected **Splunk** or **IPFIX**, from the **Forward To** list, select the destination that points to a pool of high-speed log servers to which you want the BIG-IP system to send log messages.
7. Click **Finished**.

Creating a publisher

Ensure that at least one destination associated with a pool of remote log servers exists on the BIG-IP® system.

Create a publisher to specify where the BIG-IP system sends log messages for specific resources.

1. On the Main tab, click **System** > **Logs** > **Configuration** > **Log Publishers**.
   The Log Publishers screen opens.
2. Click **Create**.
3. In the **Name** field, type a unique, identifiable name for this publisher.
4. For the **Destinations** setting, select a destination from the **Available** list, and click **<<** to move the destination to the **Selected** list.

   Note: *If you are using a formatted destination, select the destination that matches your log servers, such as Remote Syslog, Splunk, or ArcSight.*

5. Click **Finished**.

Creating a custom Protocol Security Logging profile

Create a logging profile to log Protocol Security events for the traffic handled by the virtual server to which the profile is assigned.

Note: *You can configure logging profiles for HTTP and DNS security events on Advanced Firewall Manager™, and FTP and SMTP security events on Application Security Manager™.*

1. On the Main tab, click **Security** > **Event Logs** > **Logging Profiles**.
   The Logging Profiles list screen opens.

2. Click **Create**.
   The New Logging Profile screen opens.
3. Select the **Protocol Security** check box, to enable the BIG-IP system to log HTTP, FTP, DNS, and SMTP protocol request events.
4. In the HTTP, FTP, and SMTP Security area, from the **Publisher** list, select the publisher that the BIG-IP system uses to log HTTP, FTP, and SMTP Security events.
5. In the DNS Security area, from the **Publisher** list, select the publisher that the BIG-IP system uses to log DNS Security events.
6. Select the **Log Dropped Requests** check box, to enable the BIG-IP system to log dropped DNS requests.
7. Select the **Log Filtered Dropped Requests** check box, to enable the BIG-IP system to log DNS requests dropped due to DNS query/header-opcode filtering.

   Note: *The system does not log DNS requests that are dropped due to errors in the way the system processes DNS packets.*

   ---

8. Select the **Log Malformed Requests** check box, to enable the BIG-IP system to log malformed DNS requests.
9. Select the **Log Rejected Requests** check box, to enable the BIG-IP system to log rejected DNS requests.
10. Select the **Log Malicious Requests** check box, to enable the BIG-IP system to log malicious DNS requests.
11. From the **Storage Format** list, select how the BIG-IP system formats the log. Your choices are:

Option	Description
None	Specifies the default format type in which the BIG-IP system logs messages to a remote Syslog server, for example: `"management_ip_address","bigip_hostname","context_type", "context_name","src_ip","dest_ip","src_port", "dest_port","vlan","protocol","route_domain", "acl_rule_name","action","drop_reason`
Field-List	This option allows you to: • Select from a list, the fields to be included in the log. • Specify the order the fields display in the log. • Specify the delimiter that separates the content in the log. The default delimiter is the comma character.
User-Defined	This option allows you to: • Select from a list, the fields to be included in the log. • Cut and paste, in a string of text, the order the fields display in the log.

12. Click **Finished**.

Assign this custom Protocol Security Logging profile to a virtual server.

Configuring a virtual server for Protocol Security event logging

Ensure that at least one Log Publisher exists on the BIG-IP® system.

Assign a custom Protocol Security Logging profile to a virtual server when you want the BIG-IP system to log Protocol Security events on the traffic the virtual server processes.

Note: *This task applies only to systems provisioned at a minimum level (or higher) for* ***Local Traffic (LTM)****. You can check the provisioning level on the* ***System*** *>* ***Resource Provisioning*** *screen.*

1. On the Main tab, click **Local Traffic** > **Virtual Servers**.
   The Virtual Server List screen opens.
2. Click the name of the virtual server you want to modify.
3. On the menu bar, click **Security** > **Policies**.
   The screen displays firewall rule settings.
4. From the **Log Profile** list, select **Enabled**. Then, for the **Profile** setting, move the profiles that log specific events to specific locations from the **Available** list to the **Selected** list.
5. Click **Update** to save the changes.

Disabling logging

Disable Network Firewall, Protocol Security, or DoS Protection event logging when you no longer want the BIG-IP® system to log specific events on the traffic handled by specific resources.

Note: *You can disable and re-enable logging for a specific resource based on your network administration needs.*

1. On the Main tab, click **Local Traffic** > **Virtual Servers**.
   The Virtual Server List screen opens.
2. Click the name of the virtual server you want to modify.
3. On the menu bar, click **Security** > **Policies**.
   The screen displays firewall rule settings.
4. From the **Log Profile** list, select **Disabled**.
5. Click **Update** to save the changes.

The BIG-IP system does not log the events specified in this profile for the resources to which this profile is assigned.

Implementation result

You now have an implementation in which the BIG-IP® system logs specific Protocol Security events and sends the logs to a specific location.

Configuring Remote High-Speed Logging of Network Firewall Events

Overview: Configuring remote high-speed Network Firewall event logging

You can configure the BIG-IP® system to log information about the BIG-IP system Network Firewall events and send the log messages to remote high-speed log servers.

Important: *The BIG-IP system Advanced Firewall Manager™ (AFM™) must be licensed and provisioned before you can configure Network Firewall event logging.*

When configuring remote high-speed logging of Network Firewall events, it is helpful to understand the objects you need to create and why, as described here:

Object	Reason
Pool of remote log servers	Create a pool of remote log servers to which the BIG-IP system can send log messages.
Destination (unformatted)	Create a log destination of Remote High-Speed Log type that specifies a pool of remote log servers.
Destination (formatted)	If your remote log servers are the ArcSight, Splunk, IPFIX, or Remote Syslog type, create an additional log destination to format the logs in the required format and forward the logs to a remote high-speed log destination.
Publisher	Create a log publisher to send logs to a set of specified log destinations.
Logging profile	Create a custom Logging profile to enable logging of user-specified data at a user-specified level, and associate a log publisher with the profile.
LTM® virtual server	Associate a custom Logging profile with a virtual server to define how the BIG-IP system logs security events on the traffic that the virtual server processes.

This illustration shows the association of the configuration objects for remote high-speed logging.

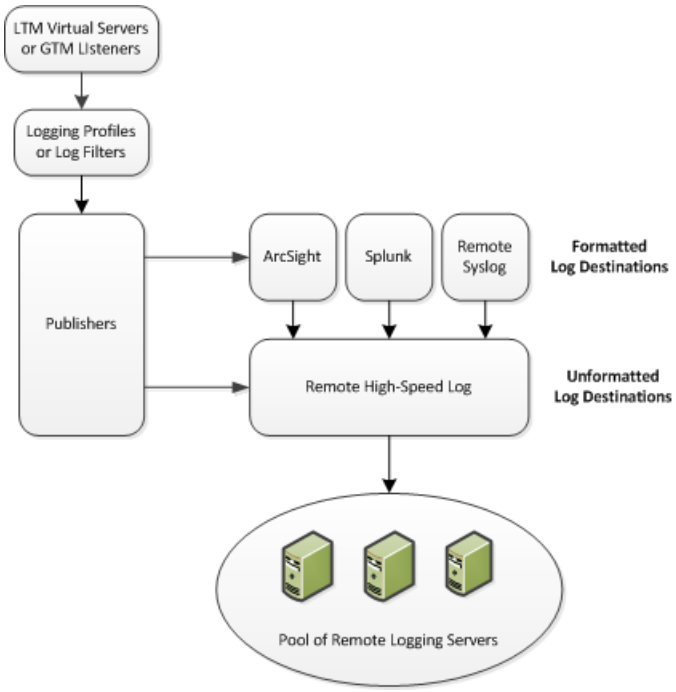

Figure 4: Association of remote high-speed logging configuration objects

Task summary

Perform these tasks to configure remote high-speed network firewall logging on the BIG-IP® system.

Note: *Enabling remote high-speed logging impacts BIG-IP system performance.*

Creating a pool of remote logging servers
Creating a remote high-speed log destination
Creating a formatted remote high-speed log destination
Creating a publisher
Creating a custom Network Firewall Logging profile
Configuring a virtual server for Network Firewall event logging
Disabling logging

Creating a pool of remote logging servers

Before creating a pool of log servers, gather the IP addresses of the servers that you want to include in the pool. Ensure that the remote log servers are configured to listen to and receive log messages from the BIG-IP® system.

Create a pool of remote log servers to which the BIG-IP system can send log messages.

1. On the Main tab, click the applicable path.
   - **DNS** > **Delivery** > **Load Balancing** > **Pools**
   - **Local Traffic** > **Pools**

   The Pool List screen opens.
2. Click **Create**.
   The New Pool screen opens.

3. In the **Name** field, type a unique name for the pool.
4. Using the **New Members** setting, add the IP address for each remote logging server that you want to include in the pool:
   a) Type an IP address in the **Address** field, or select a node address from the **Node List**.
   b) Type a service number in the **Service Port** field, or select a service name from the list.

   Note: *Typical remote logging servers require port* `514`*.*

   c) Click **Add**.
5. Click **Finished**.

Creating a remote high-speed log destination

Before creating a remote high-speed log destination, ensure that at least one pool of remote log servers exists on the BIG-IP® system.

Create a log destination of the **Remote High-Speed Log** type to specify that log messages are sent to a pool of remote log servers.

1. On the Main tab, click **System** > **Logs** > **Configuration** > **Log Destinations**.
   The Log Destinations screen opens.
2. Click **Create**.
3. In the **Name** field, type a unique, identifiable name for this destination.
4. From the **Type** list, select **Remote High-Speed Log**.

   Important: *If you use log servers such as Remote Syslog, Splunk, or ArcSight, which require data be sent to the servers in a specific format, you must create an additional log destination of the required type, and associate it with a log destination of the* ***Remote High-Speed Log*** *type. With this configuration, the BIG-IP system can send data to the servers in the required format.*

   The BIG-IP system is configured to send an unformatted string of text to the log servers.
5. From the **Pool Name** list, select the pool of remote log servers to which you want the BIG-IP system to send log messages.
6. From the **Protocol** list, select the protocol used by the high-speed logging pool members.
7. Click **Finished**.

Creating a formatted remote high-speed log destination

Ensure that at least one remote high-speed log destination exists on the BIG-IP® system.

Create a formatted logging destination to specify that log messages are sent to a pool of remote log servers, such as Remote Syslog, Splunk, or ArcSight servers.

1. On the Main tab, click **System** > **Logs** > **Configuration** > **Log Destinations**.
   The Log Destinations screen opens.
2. Click **Create**.
3. In the **Name** field, type a unique, identifiable name for this destination.

4. From the **Type** list, select a formatted logging destination, such as **IPFIX**, **Remote Syslog**, **Splunk**, or **ArcSight**.

   Important: *ArcSight formatting is only available for logs coming from Advanced Firewall Manager (AFM), Application Security Manager™ (ASM), and the Secure Web Gateway component of Access Policy Manager® (APM®). IPFIX is not available for Secure Web Gateway. Remote Syslog formatting is the only type supported for logs coming from APM. The Splunk format is a predefined format of key value pairs.*

   The BIG-IP system is configured to send a formatted string of text to the log servers.
5. If you selected **Remote Syslog**, from the **Syslog Format** list, select a format for the logs, and then from the **High-Speed Log Destination** list, select the destination that points to a pool of remote Syslog servers to which you want the BIG-IP system to send log messages.

   Important: *For logs coming from Access Policy Manager® (APM®), only the BSD Syslog format is supported.*

6. If you selected **Splunk** or **IPFIX**, from the **Forward To** list, select the destination that points to a pool of high-speed log servers to which you want the BIG-IP system to send log messages.
7. Click **Finished**.

Creating a publisher

Ensure that at least one destination associated with a pool of remote log servers exists on the BIG-IP® system.

Create a publisher to specify where the BIG-IP system sends log messages for specific resources.

1. On the Main tab, click **System** > **Logs** > **Configuration** > **Log Publishers**.
   The Log Publishers screen opens.
2. Click **Create**.
3. In the **Name** field, type a unique, identifiable name for this publisher.
4. For the **Destinations** setting, select a destination from the **Available** list, and click **<<** to move the destination to the **Selected** list.

   Note: *If you are using a formatted destination, select the destination that matches your log servers, such as Remote Syslog, Splunk, or ArcSight.*

5. Click **Finished**.

Creating a custom Network Firewall Logging profile

Create a custom Logging profile to log messages about BIG-IP® system Network Firewall events.

1. On the Main tab, click **Security** > **Event Logs** > **Logging Profiles**.
   The Logging Profiles list screen opens.
2. Click **Create**.
   The New Logging Profile screen opens.
3. In the **Name** field, type a unique name for the profile.
4. Select the **Network Firewall** check box.

5. In the Network Firewall area, from the **Publisher** list, select the publisher the BIG-IP system uses to log Network Firewall events.
6. Set an **Aggregate Rate Limit** to define a rate limit for all combined network firewall log messages per second. Beyond this rate limit, log messages are not logged.
7. For the **Log Rule Matches** setting, select how the BIG-IP system logs packets that match ACL rules. You can select any or all of the options. When an option is selected, you can configure a rate limit for log messages of that type.

Option	Description
Option	Enables or disables logging of packets that match ACL rules configured with:
Accept	`action=Accept`
Drop	`action=Drop`
Reject	`action=Reject`

8. Select the **Log IP Errors** check box, to enable logging of IP error packets. When enabled, you can configure a rate limit for log messages of this type.
9. Select the **Log TCP Errors** check box, to enable logging of TCP error packets. When enabled, you can configure a rate limit for log messages of this type.
10. Select the **Log TCP Events** check box, to enable logging of open and close of TCP sessions. When enabled, you can configure a rate limit for log messages of this type.
11. Enable the **Log Translation Fields** setting to log both the original IP address and the NAT-translated IP address for Network Firewall log events.
12. Enable the **Log Geolocation IP Address** setting to specify that when a geolocation event causes a network firewall action, the associated IP address is logged.
13. From the **Storage Format** list, select how the BIG-IP system formats the log. Your choices are:

Option	Description
None	Specifies the default format type in which the BIG-IP system logs messages to a remote Syslog server, for example: `"management_ip_address","bigip_hostname","context_type", "context_name","src_ip","dest_ip","src_port", "dest_port","vlan","protocol","route_domain", "acl_rule_name","action","drop_reason`
Field-List	This option allows you to: • Select from a list, the fields to be included in the log. • Specify the order the fields display in the log. • Specify the delimiter that separates the content in the log. The default delimiter is the comma character.
User-Defined	This option allows you to: • Select from a list, the fields to be included in the log. • Cut and paste, in a string of text, the order the fields display in the log.

14. In the IP Intelligence area, from the **Publisher** list, select the publisher that the BIG-IP system uses to log source IP addresses, which are identified and configured for logging by an IP Intelligence policy.

Note: *The IP Address Intelligence feature must be enabled and licensed.*

---

15. Set an **Aggregate Rate Limit** to define a rate limit for all combined IP Intelligence log messages per second. Beyond this rate limit, log messages are not logged.
16. Enable the **Log Translation Fields** setting to log both the original IP address and the NAT-translated IP address for IP Intelligence log events.
17. In the Traffic Statistics area, from the **Publisher** list, select the publisher that the BIG-IP system uses to log traffic statistics.
18. Enable the **Active Flows** setting to log the number of active flows each second.
19. Enable the **Reaped Flows** to log the number of reaped flows, or connections that are not established because of system resource usage levels.
20. Enable the **Missed Flows** setting to log the number of packets that were dropped because of a flow table miss. A flow table miss occurs when a TCP non-SYN packet does not match an existing flow.
21. Enable the **SYN Cookie (Per Session Challenge)**setting to log the number of SYN cookie challenges generated each second.
22. Enable the **SYN Cookie (White-listed Clients)** setting to log the number of SYN cookie clients whitelisted each second.
23. Click **Finished**.

Assign this custom network firewall Logging profile to a virtual server.

Configuring a virtual server for Network Firewall event logging

Ensure that at least one log publisher exists on the BIG-IP® system.

Assign a custom Network Firewall Logging profile to a virtual server when you want the BIG-IP system to log Network Firewall events on the traffic that the virtual server processes.

1. On the Main tab, click **Local Traffic** > **Virtual Servers**.
   The Virtual Server List screen opens.
2. Click the name of the virtual server you want to modify.
3. On the menu bar, click **Security** > **Policies**.
   The screen displays firewall rule settings.
4. From the **Log Profile** list, select **Enabled**. Then, for the **Profile** setting, move the profiles that log specific events to specific locations from the **Available** list to the **Selected** list.

   Note: *If you do not have a custom profile configured, select the predefined logging profile* ***global-network*** *to log Advanced Firewall Manager™ events. Note that to log global, self IP, and route domain contexts, you must enable a Publisher in the* ***global-network*** *profile.*

5. Click **Update** to save the changes.

Disabling logging

Disable Network Firewall, Protocol Security, or DoS Protection event logging when you no longer want the BIG-IP® system to log specific events on the traffic handled by specific resources.

Note: *You can disable and re-enable logging for a specific resource based on your network administration needs.*

1. On the Main tab, click **Local Traffic** > **Virtual Servers**.

The Virtual Server List screen opens.

2. Click the name of the virtual server you want to modify.
3. On the menu bar, click **Security** > **Policies**.
   The screen displays firewall rule settings.
4. From the **Log Profile** list, select **Disabled**.
5. Click **Update** to save the changes.

The BIG-IP system does not log the events specified in this profile for the resources to which this profile is assigned.

Implementation result

You now have an implementation in which the BIG-IP® system logs specific Network Firewall events and sends the logs to a remote log server.

Configuring Remote High-Speed Logging of DoS Protection Events

Overview: Configuring DoS Protection event logging

You can configure the BIG-IP® system to log information about BIG-IP system denial-of-service (DoS) events, and send the log messages to remote high-speed log servers.

Important: *The BIG-IP Advanced Firewall Manager™ (AFM™) must be licensed and provisioned before you can configure DoS Protection event logging. Additionally, for high-volume logging requirements, such as DoS, ensure that the BIG-IP system sends the event logs to a remote log server.*

When configuring remote high-speed logging of DoS Protection event logging, it is helpful to understand the objects you need to create and why, as described here:

Object	Reason
Pool of remote log servers	Create a pool of remote log servers to which the BIG-IP system can send log messages.
Destination (unformatted)	Create a log destination of Remote High-Speed Log type that specifies a pool of remote log servers.
Destination (formatted)	If your remote log servers are the ArcSight, Splunk, IPFIX, or Remote Syslog type, create an additional log destination to format the logs in the required format and forward the logs to a remote high-speed log destination.
Publisher	Create a log publisher to send logs to a set of specified log destinations.
Logging profile	Create a custom Logging profile to enable logging of user-specified data at a user-specified level, and associate a log publisher with the profile.
LTM® virtual server	Associate a custom Logging profile with a virtual server to define how the BIG-IP system logs security events on the traffic that the virtual server processes.

This illustration shows the association of the configuration objects for remote high-speed logging of DoS Protection events.

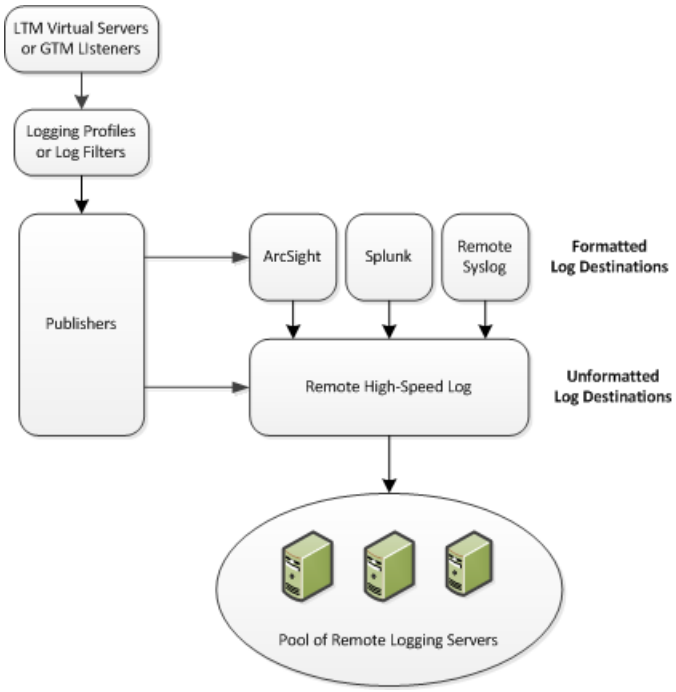

Figure 5: Association of remote high-speed logging configuration objects

Task summary

Perform these tasks to configure logging of DoS Protection events on the BIG-IP® system.

Note: *Enabling logging impacts BIG-IP system performance.*

Creating a pool of remote logging servers
Creating a remote high-speed log destination
Creating a formatted remote high-speed log destination
Creating a publisher
Creating a custom DoS Protection Logging profile
Configuring an LTM virtual server for DoS Protection event logging
Disabling logging

Creating a pool of remote logging servers

Before creating a pool of log servers, gather the IP addresses of the servers that you want to include in the pool. Ensure that the remote log servers are configured to listen to and receive log messages from the BIG-IP® system.

Create a pool of remote log servers to which the BIG-IP system can send log messages.

1. On the Main tab, click the applicable path.
   - **DNS** > **Delivery** > **Load Balancing** > **Pools**
   - **Local Traffic** > **Pools**

   The Pool List screen opens.
2. Click **Create**.
   The New Pool screen opens.

3. In the **Name** field, type a unique name for the pool.
4. Using the **New Members** setting, add the IP address for each remote logging server that you want to include in the pool:
   a) Type an IP address in the **Address** field, or select a node address from the **Node List**.
   b) Type a service number in the **Service Port** field, or select a service name from the list.

   Note: *Typical remote logging servers require port* `514`*.*

   c) Click **Add**.
5. Click **Finished**.

Creating a remote high-speed log destination

Before creating a remote high-speed log destination, ensure that at least one pool of remote log servers exists on the BIG-IP® system.

Create a log destination of the **Remote High-Speed Log** type to specify that log messages are sent to a pool of remote log servers.

1. On the Main tab, click **System** > **Logs** > **Configuration** > **Log Destinations**.
   The Log Destinations screen opens.
2. Click **Create**.
3. In the **Name** field, type a unique, identifiable name for this destination.
4. From the **Type** list, select **Remote High-Speed Log**.

   Important: *If you use log servers such as Remote Syslog, Splunk, or ArcSight, which require data be sent to the servers in a specific format, you must create an additional log destination of the required type, and associate it with a log destination of the* ***Remote High-Speed Log*** *type. With this configuration, the BIG-IP system can send data to the servers in the required format.*

   The BIG-IP system is configured to send an unformatted string of text to the log servers.
5. From the **Pool Name** list, select the pool of remote log servers to which you want the BIG-IP system to send log messages.
6. From the **Protocol** list, select the protocol used by the high-speed logging pool members.
7. Click **Finished**.

Creating a formatted remote high-speed log destination

Ensure that at least one remote high-speed log destination exists on the BIG-IP® system.

Create a formatted logging destination to specify that log messages are sent to a pool of remote log servers, such as Remote Syslog, Splunk, or ArcSight servers.

1. On the Main tab, click **System** > **Logs** > **Configuration** > **Log Destinations**.
   The Log Destinations screen opens.
2. Click **Create**.
3. In the **Name** field, type a unique, identifiable name for this destination.

4. From the **Type** list, select a formatted logging destination, such as **IPFIX**, **Remote Syslog**, **Splunk**, or **ArcSight**.

   Important: *ArcSight formatting is only available for logs coming from Advanced Firewall Manager (AFM), Application Security Manager™ (ASM), and the Secure Web Gateway component of Access Policy Manager® (APM®). IPFIX is not available for Secure Web Gateway. Remote Syslog formatting is the only type supported for logs coming from APM. The Splunk format is a predefined format of key value pairs.*

   The BIG-IP system is configured to send a formatted string of text to the log servers.
5. If you selected **Remote Syslog**, from the **Syslog Format** list, select a format for the logs, and then from the **High-Speed Log Destination** list, select the destination that points to a pool of remote Syslog servers to which you want the BIG-IP system to send log messages.

   Important: *For logs coming from Access Policy Manager® (APM®), only the BSD Syslog format is supported.*

6. If you selected **Splunk** or **IPFIX**, from the **Forward To** list, select the destination that points to a pool of high-speed log servers to which you want the BIG-IP system to send log messages.
7. Click **Finished**.

Creating a publisher

Ensure that at least one destination associated with a pool of remote log servers exists on the BIG-IP® system.

Create a publisher to specify where the BIG-IP system sends log messages for specific resources.

1. On the Main tab, click **System** > **Logs** > **Configuration** > **Log Publishers**.
   The Log Publishers screen opens.
2. Click **Create**.
3. In the **Name** field, type a unique, identifiable name for this publisher.
4. For the **Destinations** setting, select a destination from the **Available** list, and click **<<** to move the destination to the **Selected** list.

   Note: *If you are using a formatted destination, select the destination that matches your log servers, such as Remote Syslog, Splunk, or ArcSight.*

5. Click **Finished**.

Creating a custom DoS Protection Logging profile

Create a custom Logging profile to log DoS Protection events and send the log messages to a specific location.

1. On the Main tab, click **Security** > **Event Logs** > **Logging Profiles**.
   The Logging Profiles list screen opens.
2. Click **Create**.
   The New Logging Profile screen opens.
3. Select the **DoS Protection** check box.

4. In the DNS DoS Protection area, from the **Publisher** list, select the publisher that the BIG-IP system uses to log DNS DoS events.

   You can specify publishers for other DoS types in the same profile, for example, for SIP or Application DoS Protection.

5. Click **Finished**.

Assign this custom DoS Protection Logging profile to a virtual server.

Configuring an LTM virtual server for DoS Protection event logging

Ensure that at least one Log Publisher exists on the BIG-IP® system.

Assign a custom DoS Protection Logging profile to a virtual server when you want the BIG-IP system to log DoS Protection events on the traffic the virtual server processes.

Note: *This task applies only to LTM®-provisioned systems.*

---

1. On the Main tab, click **Local Traffic** > **Virtual Servers**.
   The Virtual Server List screen opens.
2. Click the name of the virtual server you want to modify.
3. On the menu bar, click **Security** > **Policies**.
   The screen displays firewall rule settings.
4. From the **Log Profile** list, select **Enabled**. Then, for the **Profile** setting, move the profiles that log specific events to specific locations from the **Available** list to the **Selected** list.
5. Click **Update** to save the changes.

Disabling logging

Disable Network Firewall, Protocol Security, or DoS Protection event logging when you no longer want the BIG-IP® system to log specific events on the traffic handled by specific resources.

Note: *You can disable and re-enable logging for a specific resource based on your network administration needs.*

---

1. On the Main tab, click **Local Traffic** > **Virtual Servers**.
   The Virtual Server List screen opens.
2. Click the name of the virtual server you want to modify.
3. On the menu bar, click **Security** > **Policies**.
   The screen displays firewall rule settings.
4. From the **Log Profile** list, select **Disabled**.
5. Click **Update** to save the changes.

The BIG-IP system does not log the events specified in this profile for the resources to which this profile is assigned.

Implementation result

You now have an implementation in which the BIG-IP® system logs specific DoS Protection events and sends the logs to a specific location.

Configuring Remote High-Speed Logging of CGNAT Processes

Overview: Configuring remote high-speed logging for CGNAT

You can configure the BIG-IP® system to log information about carrier grade network address translation (CGNAT) processes and send the log messages to remote high-speed log servers.

When configuring remote high-speed logging (HSL) of CGNAT processes, it is helpful to understand the objects you need to create and why, as described here:

Object	Reason
Pool of remote log servers	Create a pool of remote log servers to which the BIG-IP system can send log messages.
Destination (unformatted)	Create a log destination of Remote High-Speed Log type that specifies a pool of remote log servers.
Destination (formatted)	If your remote log servers are the Splunk, IPFIX, or Remote Syslog type, create an additional log destination to format the logs in the required format and forward the logs to a remote high-speed log destination.
Publisher	Create a log publisher to send logs to a set of specified log destinations.
Logging Profile (optional)	Create a logging profile to configure logging options for various large scale NAT (LSN) events. The options apply to all HSL destinations.
LSN pool	Associate an LSN pool with a logging profile and log publisher in order to log messages about the traffic that uses the pool.

This illustration shows the association of the configuration objects for remote high-speed logging of CGNAT processes.

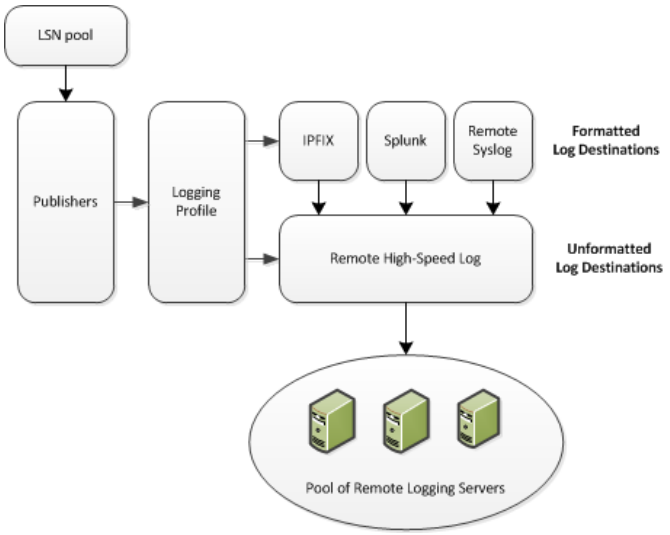

Figure 6: Association of remote high-speed logging configuration objects

Task summary

Perform these tasks to configure remote high-speed logging of CGNAT processes on the BIG-IP® system.

Note: *Enabling remote high-speed logging impacts BIG-IP system performance.*

Creating a pool of remote logging servers
Creating a remote high-speed log destination
Creating a formatted remote high-speed log destination
Creating a publisher
Creating an LSN logging profile
Configuring an LSN pool

Creating a pool of remote logging servers

Before creating a pool of log servers, gather the IP addresses of the servers that you want to include in the pool. Ensure that the remote log servers are configured to listen to and receive log messages from the BIG-IP® system.

Create a pool of remote log servers to which the BIG-IP system can send log messages.

1. On the Main tab, click the applicable path.
   - **DNS** > **Delivery** > **Load Balancing** > **Pools**
   - **Local Traffic** > **Pools**

   The Pool List screen opens.
2. Click **Create**.
   The New Pool screen opens.
3. In the **Name** field, type a unique name for the pool.
4. Using the **New Members** setting, add the IP address for each remote logging server that you want to include in the pool:
   a) Type an IP address in the **Address** field, or select a node address from the **Node List**.
   b) Type a service number in the **Service Port** field, or select a service name from the list.

Note: *Typical remote logging servers require port* `514`*.*

c) Click **Add**.

5. Click **Finished**.

Creating a remote high-speed log destination

Before creating a remote high-speed log destination, ensure that at least one pool of remote log servers exists on the BIG-IP® system.

Create a log destination of the **Remote High-Speed Log** type to specify that log messages are sent to a pool of remote log servers.

1. On the Main tab, click **System** > **Logs** > **Configuration** > **Log Destinations**.
   The Log Destinations screen opens.
2. Click **Create**.
3. In the **Name** field, type a unique, identifiable name for this destination.
4. From the **Type** list, select **Remote High-Speed Log**.

   Important: *If you use log servers such as Remote Syslog, Splunk, or IPFIX, which require data be sent to the servers in a specific format, you must create an additional log destination of the required type, and associate it with a log destination of the* ***Remote High-Speed Log*** *type. This allows the BIG-IP system to send data to the servers in the required format.*

   The BIG-IP system is configured to send an unformatted string of text to the log servers.
5. From the **Pool Name** list, select the pool of remote log servers to which you want the BIG-IP system to send log messages.
6. From the **Protocol** list, select the protocol used by the high-speed logging pool members.
7. Click **Finished**.

Creating a formatted remote high-speed log destination

Ensure that at least one remote high-speed log destination exists on the BIG-IP® system.

Create a formatted logging destination to specify that log messages are sent to a pool of remote log servers, such as Remote Syslog, Splunk, or IPFIX servers.

1. On the Main tab, click **System** > **Logs** > **Configuration** > **Log Destinations**.
   The Log Destinations screen opens.
2. Click **Create**.
3. In the **Name** field, type a unique, identifiable name for this destination.
4. From the **Type** list, select a formatted logging destination, such as **Remote Syslog**, **Splunk**, or **IPFIX**.

   The Splunk format is a predefined format of key value pairs.

   The BIG-IP system is configured to send a formatted string of text to the log servers.
5. If you selected **Remote Syslog**, from the **Syslog Format** list, select a format for the logs, and then from the **High-Speed Log Destination** list, select the destination that points to a pool of remote Syslog servers to which you want the BIG-IP system to send log messages.

Important: *For logs coming from Access Policy Manager® (APM®), only the BSD Syslog format is supported.*

6. If you selected **Splunk** or **IPFIX**, from the **Forward To** list, select the destination that points to a pool of high-speed log servers to which you want the BIG-IP system to send log messages.
7. Click **Finished**.

Creating a publisher

Ensure that at least one destination associated with a pool of remote log servers exists on the BIG-IP® system.

Create a publisher to specify where the BIG-IP system sends log messages for specific resources.

1. On the Main tab, click **System** > **Logs** > **Configuration** > **Log Publishers**.
   The Log Publishers screen opens.
2. Click **Create**.
3. In the **Name** field, type a unique, identifiable name for this publisher.
4. For the **Destinations** setting, select a destination from the **Available** list, and click **<<** to move the destination to the **Selected** list.

Note: *If you are using a formatted destination, select the destination that matches your log servers, such as Remote Syslog, Splunk, or IPFIX.*

Important: *If you configure a log publisher to use multiple logging destinations, then, by default, all logging destinations must be available in order to log to each destination. Unless all logging destinations are available, no logging can occur. If you want to log to the available logging destinations when one or more destinations become unavailable, you must set the* `logpublisher.atomic` *db variable to* `false`.

5. Click **Finished**.

Creating an LSN logging profile

You can create an LSN logging profile to allow you to configure logging options for various LSN events that apply to high-speed logging destinations.

Note: *For configuring remote high-speed logging of CGNAT processes on the BIG-IP® system, these steps are optional.*

1. On the Main tab, click **Carrier Grade NAT** > **Logging Profiles** > **LSN**.
   The LSN logging profiles screen opens.
2. Click **Create**.
   The New LSN Logging Profile screen opens.
3. In the **Name** field, type a unique name for the logging profile.
4. From the **Parent Profile** list, select a profile from which the new profile inherits properties.
5. Select the **Custom** check box for the Log Settings area.
6. For the Log Settings area, select **Enabled** for the following settings, as necessary.

Setting	Description
Start Outbound Session	Generates event log entries at the start of a translation event for an LSN client.
End Outbound Session	Generates event log entries at the end of a translation event for an LSN client.
Start Inbound Session	Generates event log entries at the start of an incoming connection event for a translated endpoint.
End Inbound Session	Generates event log entries at the end of an incoming connection event for a translated endpoint.
Quota Exceeded	Generates event log entries when an LSN client exceeds allocated resources.
Errors	Generates event log entries when LSN translation errors occur.

7. Click **Finished**.

Configuring an LSN pool

You can associate an LSN pool with a log publisher and logging profile that the BIG-IP® system uses to send log messages to a specified destination.

1. On the Main tab, click **Carrier Grade NAT** > **LSN Pools** > **LSN Pool List**.
   The LSN Pool List screen opens.
2. Select an LSN pool from the list.
   The configuration screen for the pool opens.
3. From the **Log Publisher** list, select the log publisher the BIG-IP system uses to send log messages to a specified destination.

   Important: *If you configure a log publisher to use multiple logging destinations, then, by default, all logging destinations must be available in order to log to each destination. Unless all logging destinations are available, no logging can occur. If you want to log to the available logging destinations when one or more destinations become unavailable, you must set the* `logpublisher.atomic` *db variable to* `false`.

4. Optional: From the **Logging Profile** list, select the logging profile the BIG-IP system uses to configure logging options for various LSN events.
5. Click **Finished**.

You now have an LSN pool for which the BIG-IP system logs messages using the specified logging profile.

Configuring CGNAT IPFIX Logging

Overview: Configuring IPFIX logging for CGNAT

You can configure the BIG-IP® system to log information about carrier grade network address translation (CGNAT) processes and send the log messages to remote IPFIX collectors.

IPFIX is a set of IETF standards described in RFCs 5101 and 5102. The BIG-IP system supports logging of CGNAT translation events over the IPFIX protocol. 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.

The configuration process involves creating and connecting the following configuration objects.

Object	Reason
Pool of IPFIX collectors	Create a pool of IPFIX collectors to which the BIG-IP system can send IPFIX log messages.
Destination	Create a log destination to format the logs in IPFIX templates, and forward the logs to the IPFIX collectors.
Publisher	Create a log publisher to send logs to a set of specified log destinations.
Logging Profile (optional)	Create a logging profile to configure logging options for various large scale NAT (LSN) events. The options apply to all HSL destinations.
LSN pool	Associate an LSN pool with a logging profile and log publisher in order to log messages about the traffic that uses the pool.

This illustration shows the association of the configuration objects for IPFIX logging of CGNAT processes.

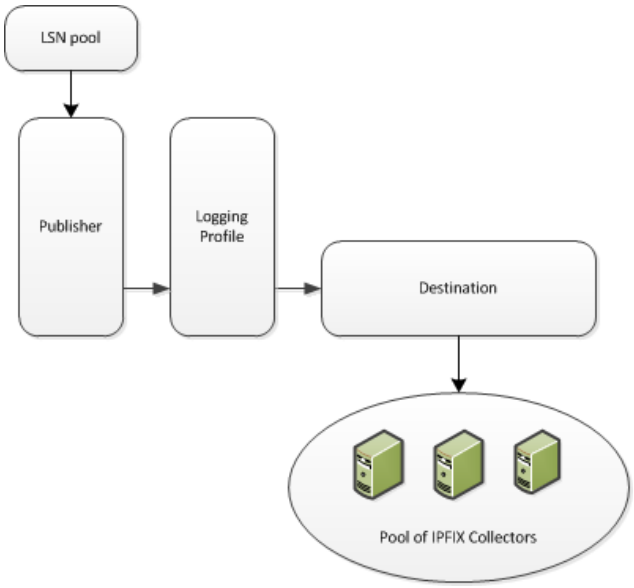

Figure 7: Association of logging configuration objects

Task summary

Perform these tasks to configure IPFIX logging of CGNAT processes on the BIG-IP system.

Note: *Enabling IPFIX logging impacts BIG-IP system performance.*

Assembling a pool of IPFIX collectors
Creating an IPFIX log destination
Creating a publisher
Creating an LSN logging profile
Configuring an LSN pool

Assembling a pool of IPFIX collectors

Before creating a pool of IPFIX collectors, gather the IP addresses of the collectors that you want to include in the pool. Ensure that the remote IPFIX collectors are configured to listen to and receive log messages from the BIG-IP® system.

These are the steps for creating a pool of IPFIX collectors. The BIG-IP system can send IPFIX log messages to this pool.

1. On the Main tab, click **Local Traffic** > **Pools**.
   The Pool List screen opens.
2. Click **Create**.
   The New Pool screen opens.
3. In the **Name** field, type a unique name for the pool.
4. Using the **New Members** setting, add the IP address for each IPFIX collector that you want to include in the pool:
   a) Type the collector's IP address in the **Address** field, or select a node address from the **Node List**.
   b) Type a port number in the **Service Port** field.
   By default, IPFIX collectors listen on UDP or TCP port `4739` and Netflow V9 devices listen on port `2055`, though the port is configurable at each collector.

c) Click **Add**.

5. Click **Finished**.

Creating an IPFIX log destination

A log destination of the **IPFIX** type specifies that log messages are sent to a pool of IPFIX collectors. Use these steps to create a log destination for IPFIX collectors.

1. On the Main tab, click **System** > **Logs** > **Configuration** > **Log Destinations**.
   The Log Destinations screen opens.
2. Click **Create**.
3. In the **Name** field, type a unique, identifiable name for this destination.
4. From the **Type** list, select **IPFIX**.
5. From the **Protocol** list, select **IPFIX** or **Netflow V9**, depending on the type of collectors you have in the pool.
6. From the **Pool Name** list, select an LTM® pool of IPFIX collectors.
7. From the **Transport Profile** list, select **TCP**, **UDP**, or any customized profile derived from TCP or UDP.
8. The **Template Retransmit Interval** is the time between transmissions of IPFIX templates to the pool of collectors. The BIG-IP system only retransmits its templates if the **Transport Profile** is a **UDP** profile.

   An *IPFIX template* defines the field types and byte lengths of the binary IPFIX log messages. The logging destination sends the template for a given log type (for example, NAT44 logs or customized logs from an iRule) before sending any of those logs, so that the IPFIX collector can read the logs of that type. The logging destination assigns a template ID to each template, and places the template ID into each log that uses that template.

   The log destination periodically retransmits all of its IPFIX templates over a UDP connection. The retransmissions are helpful for UDP connections, which are lossy.
9. The **Template Delete Delay** is the time that the BIG-IP device should pause between deleting an obsolete template and re-using its template ID. This feature is helpful for systems that can create custom IPFIX templates with iRules.
10. The **Server SSL Profile** applies Secure Socket Layer (SSL) or Transport Layer Security (TLS) to TCP connections. You can only choose an SSL profile if the **Transport Profile** is a **TCP** profile. Choose an SSL profile that is appropriate for the IPFIX collectors' SSL/TLS configuration.

    SSL or TLS requires extra processing and therefore slows the connection, so we only recommend this for sites where the connections to the IPFIX collectors have a potential security risk.
11. Click **Finished**.

Creating a publisher

A publisher specifies where the BIG-IP® system sends log messages for IPFIX logs.

1. On the Main tab, click **System** > **Logs** > **Configuration** > **Log Publishers**.
   The Log Publishers screen opens.
2. Click **Create**.
3. In the **Name** field, type a unique, identifiable name for this publisher.

4. Use the Log Destinations area to select an existing IPFIX destination (perhaps along with other destinations for your logs): click any destination name in the **Available** list, and click **<<** to move it to the **Selected** list.
5. Click **Finished**.

Creating an LSN logging profile

You can create an LSN logging profile to allow you to configure logging options for various LSN events that apply to IPFIX logging destinations.

Note: *For configuring IPFIX logging of CGNAT processes on the BIG-IP® system, these steps are optional.*

1. On the Main tab, click **Carrier Grade NAT** > **Logging Profiles** > **LSN**.
   The LSN profile list screen opens.
2. Click **Create**.
   The New LSN Logging Profile screen opens.
3. In the **Name** field, type a unique name for the logging profile.
4. From the **Parent Profile** list, select a profile from which the new profile inherits properties.
5. Select the **Custom** check box for the Log Settings area.
6. For the Log Settings area, select **Enabled** for the following settings, as necessary.

Setting	Description
Start Outbound Session	Generates event log entries at the start of a translation event for an LSN client.
End Outbound Session	Generates event log entries at the end of a translation event for an LSN client.
Start Inbound Session	Generates event log entries at the start of an incoming connection event for a translated endpoint.
End Inbound Session	Generates event log entries at the end of an incoming connection event for a translated endpoint.
Quota Exceeded	Generates event log entries when an LSN client exceeds allocated resources.
Errors	Generates event log entries when LSN translation errors occur.

7. Click **Finished**.

Configuring an LSN pool

You can associate an LSN pool with a log publisher and logging profile that the BIG-IP® system uses to send log messages to a specified destination.

1. On the Main tab, click **Carrier Grade NAT** > **LSN Pools** > **LSN Pool List**.
   The LSN Pool List screen opens.
2. Select an LSN pool from the list.
   The configuration screen for the pool opens.

3. From the **Log Publisher** list, select the log publisher the BIG-IP system uses to send log messages to a specified destination.

   Important: *If you configure a log publisher to use multiple logging destinations, then, by default, all logging destinations must be available in order to log to each destination. Unless all logging destinations are available, no logging can occur. If you want to log to the available logging destinations when one or more destinations become unavailable, you must set the* `logpublisher.atomic` *db variable to* `false`*.*

4. Optional: From the **Logging Profile** list, select the logging profile the BIG-IP system uses to configure logging options for various LSN events.
5. Click **Finished**.

You now have an LSN pool for which the BIG-IP system logs messages using the specified logging profile.

Logging Network Firewall Events to IPFIX Collectors

Overview: Configuring IPFIX logging for AFM

You can configure the BIG-IP® system to log information about Advanced Firewall Manager™ (AFM™) processes and send the log messages to remote IPFIX collectors.

The BIG-IP system supports logging of AFM events over the IPFIX protocol. 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.

The configuration process involves creating and connecting the following configuration objects:

Object	Reason
Pool of IPFIX collectors	Create a pool of IPFIX collectors to which the BIG-IP system can send IPFIX log messages.
Destination	Create a log destination to format the logs in IPFIX templates, and forward the logs to the IPFIX collectors.
Publisher	Create a log publisher to send logs to a set of specified log destinations.

Task summary

Perform these tasks to configure IPFIX logging of AFM processes on the BIG-IP® system.

Note: *Enabling IPFIX logging impacts BIG-IP system performance.*

Assembling a pool of IPFIX collectors
Creating an IPFIX log destination
Creating a publisher
Creating a custom Network Firewall Logging profile
Configuring an LTM virtual server for Network Firewall event logging with IPFIX

Assembling a pool of IPFIX collectors

Before creating a pool of IPFIX collectors, gather the IP addresses of the collectors that you want to include in the pool. Ensure that the remote IPFIX collectors are configured to listen to and receive log messages from the BIG-IP® system.

These are the steps for creating a pool of IPFIX collectors. The BIG-IP system can send IPFIX log messages to this pool.

1. On the Main tab, click **Local Traffic** > **Pools**.
   The Pool List screen opens.
2. Click **Create**.
   The New Pool screen opens.

3. In the **Name** field, type a unique name for the pool.
4. Using the **New Members** setting, add the IP address for each IPFIX collector that you want to include in the pool:
   a) Type the collector's IP address in the **Address** field, or select a node address from the **Node List**.
   b) Type a port number in the **Service Port** field.

      By default, IPFIX collectors listen on UDP or TCP port `4739` and Netflow V9 devices listen on port `2055`, though the port is configurable at each collector.

   c) Click **Add**.
5. Click **Finished**.

Creating an IPFIX log destination

A log destination of the **IPFIX** type specifies that log messages are sent to a pool of IPFIX collectors. Use these steps to create a log destination for IPFIX collectors.

1. On the Main tab, click **System** > **Logs** > **Configuration** > **Log Destinations**.
   The Log Destinations screen opens.
2. Click **Create**.
3. In the **Name** field, type a unique, identifiable name for this destination.
4. From the **Type** list, select **IPFIX**.
5. From the **Protocol** list, select **IPFIX** or **Netflow V9**, depending on the type of collectors you have in the pool.
6. From the **Pool Name** list, select an LTM® pool of IPFIX collectors.
7. From the **Transport Profile** list, select **TCP**, **UDP**, or any customized profile derived from TCP or UDP.
8. The **Template Retransmit Interval** is the time between transmissions of IPFIX templates to the pool of collectors. The BIG-IP system only retransmits its templates if the **Transport Profile** is a **UDP** profile.

   An *IPFIX template* defines the field types and byte lengths of the binary IPFIX log messages. The logging destination sends the template for a given log type (for example, NAT44 logs or customized logs from an iRule) before sending any of those logs, so that the IPFIX collector can read the logs of that type. The logging destination assigns a template ID to each template, and places the template ID into each log that uses that template.

   The log destination periodically retransmits all of its IPFIX templates over a UDP connection. The retransmissions are helpful for UDP connections, which are lossy.
9. The **Template Delete Delay** is the time that the BIG-IP device should pause between deleting an obsolete template and re-using its template ID. This feature is helpful for systems that can create custom IPFIX templates with iRules.
10. The **Server SSL Profile** applies Secure Socket Layer (SSL) or Transport Layer Security (TLS) to TCP connections. You can only choose an SSL profile if the **Transport Profile** is a **TCP** profile. Choose an SSL profile that is appropriate for the IPFIX collectors' SSL/TLS configuration.

    SSL or TLS requires extra processing and therefore slows the connection, so we only recommend this for sites where the connections to the IPFIX collectors have a potential security risk.
11. Click **Finished**.

Creating a publisher

A publisher specifies where the BIG-IP® system sends log messages for IPFIX logs.

1. On the Main tab, click **System** > **Logs** > **Configuration** > **Log Publishers**.
   The Log Publishers screen opens.
2. Click **Create**.
3. In the **Name** field, type a unique, identifiable name for this publisher.
4. Use the Log Destinations area to select an existing IPFIX destination (perhaps along with other destinations for your logs): click any destination name in the **Available** list, and click **<<** to move it to the **Selected** list.
5. Click **Finished**.

Creating a custom Network Firewall Logging profile

Create a custom Logging profile to log messages about BIG-IP® system Network Firewall events.

1. On the Main tab, click **Security** > **Event Logs** > **Logging Profiles**.
   The Logging Profiles list screen opens.
2. Click **Create**.
   The New Logging Profile screen opens.
3. In the **Name** field, type a unique name for the profile.
4. Select the **Network Firewall** check box.
5. In the Network Firewall area, from the **Publisher** list, select the publisher the BIG-IP system uses to log Network Firewall events.
6. Set an **Aggregate Rate Limit** to define a rate limit for all combined network firewall log messages per second. Beyond this rate limit, log messages are not logged.
7. For the **Log Rule Matches** setting, select how the BIG-IP system logs packets that match ACL rules. You can select any or all of the options. When an option is selected, you can configure a rate limit for log messages of that type.

Option	Description
Option	Enables or disables logging of packets that match ACL rules configured with:
Accept	`action=Accept`
Drop	`action=Drop`
Reject	`action=Reject`

8. Select the **Log IP Errors** check box, to enable logging of IP error packets. When enabled, you can configure a rate limit for log messages of this type.
9. Select the **Log TCP Errors** check box, to enable logging of TCP error packets. When enabled, you can configure a rate limit for log messages of this type.
10. Select the **Log TCP Events** check box, to enable logging of open and close of TCP sessions. When enabled, you can configure a rate limit for log messages of this type.
11. Enable the **Log Translation Fields** setting to log both the original IP address and the NAT-translated IP address for Network Firewall log events.

12. Enable the **Log Geolocation IP Address** setting to specify that when a geolocation event causes a network firewall action, the associated IP address is logged.
13. From the **Storage Format** list, select how the BIG-IP system formats the log. Your choices are:

Option	Description
None	Specifies the default format type in which the BIG-IP system logs messages to a remote Syslog server, for example: `"management_ip_address","bigip_hostname","context_type", "context_name","src_ip","dest_ip","src_port", "dest_port","vlan","protocol","route_domain", "acl_rule_name","action","drop_reason`
Field-List	This option allows you to: • Select from a list, the fields to be included in the log. • Specify the order the fields display in the log. • Specify the delimiter that separates the content in the log. The default delimiter is the comma character.
User-Defined	This option allows you to: • Select from a list, the fields to be included in the log. • Cut and paste, in a string of text, the order the fields display in the log.

14. In the IP Intelligence area, from the **Publisher** list, select the publisher that the BIG-IP system uses to log source IP addresses, which are identified and configured for logging by an IP Intelligence policy.

Note: *The IP Address Intelligence feature must be enabled and licensed.*

---

15. Set an **Aggregate Rate Limit** to define a rate limit for all combined IP Intelligence log messages per second. Beyond this rate limit, log messages are not logged.
16. Enable the **Log Translation Fields** setting to log both the original IP address and the NAT-translated IP address for IP Intelligence log events.
17. In the Traffic Statistics area, from the **Publisher** list, select the publisher that the BIG-IP system uses to log traffic statistics.
18. Enable the **Active Flows** setting to log the number of active flows each second.
19. Enable the **Reaped Flows** to log the number of reaped flows, or connections that are not established because of system resource usage levels.
20. Enable the **Missed Flows** setting to log the number of packets that were dropped because of a flow table miss. A flow table miss occurs when a TCP non-SYN packet does not match an existing flow.
21. Enable the **SYN Cookie (Per Session Challenge)**setting to log the number of SYN cookie challenges generated each second.
22. Enable the **SYN Cookie (White-listed Clients)** setting to log the number of SYN cookie clients whitelisted each second.
23. Click **Finished**.

Assign this custom network firewall Logging profile to a virtual server.

Configuring an LTM virtual server for Network Firewall event logging with IPFIX

Ensure that at least one log publisher exists on the BIG-IP® system.

Assign a custom Network Firewall Logging profile to a virtual server when you want the BIG-IP system to log Network Firewall events to IPFIX collectors on the traffic that the virtual server processes.

Note: *This task applies only to LTM®-provisioned systems.*

1. On the Main tab, click **Local Traffic** > **Virtual Servers**.
   The Virtual Server List screen opens.
2. Click the name of the virtual server you want to modify.
3. On the menu bar, click **Security** > **Policies**.
   The screen displays firewall rule settings.
4. From the **Log Profile** list, select **Enabled**. Then, for the **Profile** setting, move the profiles that log specific events to IPFIX collectors from the **Available** list to the **Selected** list.

   Note: *To log global, self IP, and route domain contexts, you must enable a Publisher in the* ***global-network*** *profile.*

5. Click **Update** to save the changes.

Overview: Configuring IPFIX logging for AFM
Creating a custom Network Firewall Logging profile
Overview: Customizing IPFIX logging with iRules

Implementation result

Now you have an implementation in which the BIG-IP® system logs messages about AFM™ events and sends the log messages to a pool of IPFIX collectors.

Note: *Network firewall events are logged only for rules or policies for which logging is enabled.*

Customizing IPFIX Logging with iRules

Overview: Customizing IPFIX logging with iRules

You can configure iRules® to parse incoming packets and create IPFIX logs for them.

The BIG-IP® system supports logging of any network events over the IPFIX protocol. An iRule matches any network event that you choose and creates a customized IPFIX log from the given event.

The IPFIX logs use the information model described in RFC 5102. 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 logs.

The configuration process involves creating and connecting the following configuration objects.

Object	Reason
Pool of IPFIX collectors	Create a pool of IPFIX collectors to which the BIG-IP system can send IPFIX log messages.
Destination	Create a log destination to format the logs in IPFIX templates, and forward the logs to the IPFIX collectors.
Publisher	Create a log publisher to send logs to a set of specified log destinations.
iRule	Create an iRule that matches a network event, creates an IPFIX log to record the event, and sends the IPFIX log to the above publisher.
Virtual Server	Create a virtual server to process network traffic, or edit an existing virtual server. Add the iRule to the virtual-server configuration so that the iRule parses all of the virtual server's network traffic.

This illustration shows the association of the configuration objects for IPFIX logging through iRules.

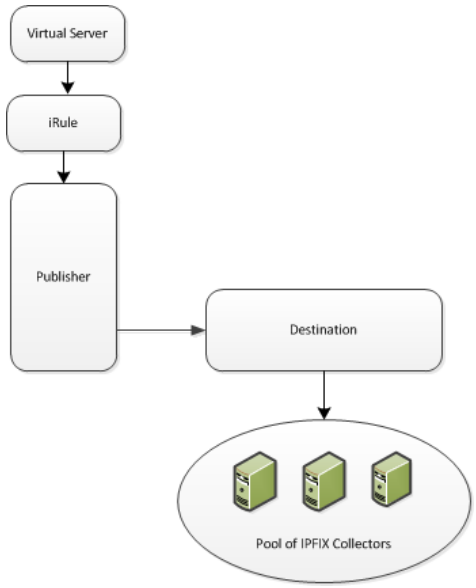

Figure 8: Association of logging configuration objects

Task summary

Perform these tasks to configure iRules for IPFIX logging.

Note: *Enabling IPFIX logging impacts BIG-IP system performance.*

Assembling a pool of IPFIX collectors
Creating an IPFIX log destination
Creating a publisher
About standard IPFIX elements
Writing an iRule for custom IPFIX logging
Adding the iRule to a virtual server
Showing IPFIX statistics
Advanced IPFIX iRule tasks

Assembling a pool of IPFIX collectors

Before creating a pool of IPFIX collectors, gather the IP addresses of the collectors that you want to include in the pool. Ensure that the remote IPFIX collectors are configured to listen to and receive log messages from the BIG-IP® system.

These are the steps for creating a pool of IPFIX collectors. The BIG-IP system can send IPFIX log messages to this pool.

1. On the Main tab, click **Local Traffic** > **Pools**.
   The Pool List screen opens.
2. Click **Create**.
   The New Pool screen opens.
3. In the **Name** field, type a unique name for the pool.
4. Using the **New Members** setting, add the IP address for each IPFIX collector that you want to include in the pool:
   a) Type the collector's IP address in the **Address** field, or select a node address from the **Node List**.

b) Type a port number in the **Service Port** field.

By default, IPFIX collectors listen on UDP or TCP port `4739` and Netflow V9 devices listen on port `2055`, though the port is configurable at each collector.

c) Click **Add**.

5. Click **Finished**.

Creating an IPFIX log destination

A log destination of the **IPFIX** type specifies that log messages are sent to a pool of IPFIX collectors. Use these steps to create a log destination for IPFIX collectors.

1. On the Main tab, click **System** > **Logs** > **Configuration** > **Log Destinations**.
   The Log Destinations screen opens.
2. Click **Create**.
3. In the **Name** field, type a unique, identifiable name for this destination.
4. From the **Type** list, select **IPFIX**.
5. From the **Protocol** list, select **IPFIX** or **Netflow V9**, depending on the type of collectors you have in the pool.
6. From the **Pool Name** list, select an LTM® pool of IPFIX collectors.
7. From the **Transport Profile** list, select **TCP**, **UDP**, or any customized profile derived from TCP or UDP.
8. The **Template Retransmit Interval** is the time between transmissions of IPFIX templates to the pool of collectors. The BIG-IP system only retransmits its templates if the **Transport Profile** is a **UDP** profile.

   An *IPFIX template* defines the field types and byte lengths of the binary IPFIX log messages. The logging destination sends the template for a given log type (for example, NAT44 logs or customized logs from an iRule) before sending any of those logs, so that the IPFIX collector can read the logs of that type. The logging destination assigns a template ID to each template, and places the template ID into each log that uses that template.

   The log destination periodically retransmits all of its IPFIX templates over a UDP connection. The retransmissions are helpful for UDP connections, which are lossy.
9. The **Template Delete Delay** is the time that the BIG-IP device should pause between deleting an obsolete template and re-using its template ID. This feature is helpful for systems that can create custom IPFIX templates with iRules.
10. The **Server SSL Profile** applies Secure Socket Layer (SSL) or Transport Layer Security (TLS) to TCP connections. You can only choose an SSL profile if the **Transport Profile** is a **TCP** profile. Choose an SSL profile that is appropriate for the IPFIX collectors' SSL/TLS configuration.

    SSL or TLS requires extra processing and therefore slows the connection, so we only recommend this for sites where the connections to the IPFIX collectors have a potential security risk.
11. Click **Finished**.

Creating a publisher

A publisher specifies where the BIG-IP® system sends log messages for IPFIX logs.

1. On the Main tab, click **System** > **Logs** > **Configuration** > **Log Publishers**.
   The Log Publishers screen opens.

2. Click **Create**.
3. In the **Name** field, type a unique, identifiable name for this publisher.
4. Use the Log Destinations area to select an existing IPFIX destination (perhaps along with other destinations for your logs): click any destination name in the **Available** list, and click **<<** to move it to the **Selected** list.
5. Click **Finished**.

About standard IPFIX elements

The BIG-IP® software is shipped with the latest Information Elements (IEs) published by IANA. Each standard element is built into the system. You can use a standard element in your iRules® by using its name and a `":base"` extension (for example, `"deltaFlowCount:base"` or `"observationTimeSeconds:base"`).

You can use this `tmsh` command to identify the available base IEs on the system:

```
list sys ipfix element
```

If an element is defined by IANA after the BIG-IP software is built, the element is not available in the system software. You can use a similar `tmsh` command, `create sys ipfix element ...`, to create such an element and use it in your iRules.

Writing an iRule for custom IPFIX logging

Before you begin, you must have a log destination that leads to a pool of IPFIX collectors.

You can create an iRule that reads network packets and logs information about them to your IPFIX collectors. Each iRule must take the following steps:

1. Open an IPFIX::destination.
2. Create an IPFIX::template.
3. Create an IPFIX::msg (using the IPFIX::template).
4. Set values for the IPFIX elements in the IPFIX::msg.
5. Send the IPFIX::msg to the IPFIX::destination.

Follow these steps to create all of these components.

1. On the Main tab, click **Local Traffic** > **iRules**.
   The iRule List screen displays a list of existing iRules®.
2. Click the **Create** button.
   The New iRule screen opens.
3. In the **Name** field, type a unique name for the iRule.
4. In the **Definition** field, type an iRule to match IP fields and log an IPFIX message based on their settings. You can use standard IPFIX elements.

   These sub-steps explain how to create all of the necessary iRule components.

   a) Open a new IPFIX::destination, which is a pre-created log publisher, with the following syntax:

   ```
   <ipfix_dest_handle> = IPFIX::destination open -publisher <logging_publisher>
   ```

   This returns a destination handle to be used later. The `<logging_publisher>` is required; this must already exist and include a pool of IPFIX collectors. This is a partition path to the publisher configuration, such as `/Common/myPublisher`.

Note: *Use a unique name for the variable that holds this handle. If two or more iRules in the same virtual server reference a variable with the same name, the results at run-time are unpredictable. Use the rule name in all of this rule's variables; do this once per destination in the iRule, and store all destinations in static variables. Every message that goes to a particular destination can reference the same static destination handle. Create this and initialize it to empty ("") in the RULE_INIT event.*

---

b) Create a new IPFIX::template with the following syntax:

```
<ipfix_template_handle> = IPFIX::template create "<element_name>
<element_name> ... <element_name>"
```

This returns a template handle to be used in later `IPFIX::msg` commands. At least one `<element_name>` is required, and each element name must be defined through IANA or through `tmsh` commands. The element order you use here is the order of the IPFIX template. You can use the same element multiple times.

Note: *As with destination variables, template variables must have unique names across all iRules.*

Do this once per template in the iRule, and store all templates in static variables. Every message that uses the template can reference the same static template handle. Create this an initialize it to empty ("") in the RULE_INIT event.

c) When you match an interesting event, create a new IPFIX::msg with the following syntax:

```
<ipfix_message_handle> = IPFIX::msg create <ipfix_template_handle>
```

This returns a message handle to be used in later IPFIX::msg commands. Use an <ipfix_template_handle> you created with an earlier IPFIX::template command. This starts the creation of an IPFIX message using the given IPFIX template.

Note: *Choose a unique name for the message across all iRules.*

---

d) Later in the same IP event, add interesting data the IPFIX::msg with the following syntax:

```
IPFIX::msg set <ipfix_message_handle> <element_name> [-pos <position>]
<value>
```

- **<ipfix_message_handle>** is an IPFIX::msg you created earlier.
- **<element_name>** is the name of an element in the message's IPFIX::template.
- **-pos <position>** (optional) only applies to an element that appears more than once in the template. The first instance of an element is element zero. If you omit this, the system applies the value to the first instance of the element (instance zero).
- **<value>** sets the value of the element.

If you use this command on the same element position more than once, the final setting overwrites the previous settings.

e) Send the finished IPFIX::msg to an IPFIX::destination, using the following syntax:

```
IPFIX::destination send <ipfix_dest_handle> <ipfix_message_handle>
```

For example, this iRule matches an HTTP exchange and sends a log about its basic parameters to IPFIX collectors:

```
# This rule captures HTTP traffic and sends logs to IPFIX collectors.

  when RULE_INIT {
    set static::http_rule1_dest ""
    set static::http_rule1_tmplt ""
  }
```

```
  when CLIENT_ACCEPTED {
    if { $static::http_rule1_dest == ""} {
      # open the logging destination if it has not been opened yet
      set static::http_rule1_dest [IPFIX::destination open -publisher
/Common/ipfix_publisher]
    }

    if { $static::http_rule1_tmplt == ""} {
      # if the template has not been created yet, create the template
     set static::http_rule1_tmplt [IPFIX::template create "flowStartSeconds
 sourceIPv4Address tcpSourcePort flowDurationMilliseconds"]
     }
  }

  when HTTP_REQUEST {
    # create a new message for this request
    set rule1_msg1 [IPFIX::msg create $static::http_rule1_tmplt]

    # compose the IPFIX log message
    IPFIX::msg set $rule1_msg1 flowStartSeconds [clock seconds]
    IPFIX::msg set $rule1_msg1 sourceIPv4Address [IP::client_addr]
    IPFIX::msg set $rule1_msg1 tcpSourcePort [TCP::client_port]

    # record the start time in milliseconds
    set start [clock clicks -milliseconds]
  }

  when HTTP_RESPONSE_RELEASE {
    # figure out the final duration and add it to the IPFIX log
    set stop [expr {[clock click -milliseconds] - $start}]
    IPFIX::msg set $rule1_msg1 flowDurationMilliseconds $stop

    # send the IPFIX log
    IPFIX::destination send $static::http_rule1_dest $rule1_msg1
  }
}
```

5. Click **Finished**.

The iRule is now available. You can use this iRule in a virtual server that serves HTTP clients.

Adding the iRule to a virtual server

After you create a pool of collectors, logging components, IPFIX elements (optionally), and an iRule, you need to create a virtual server that references those components.

1. On the Main tab, click **Local Traffic** > **Virtual Servers**.
   The Virtual Server List screen opens.
2. Click the name of the virtual server you want to modify.
3. On the menu bar, click **Resources**.
4. For the **iRules** setting, from the **Available** list, select the name of the iRule that creates custom IPFIX logs. Move the name into the **Enabled** list.
5. Click **Finished**.

The virtual server is configured to use the iRule for IPFIX logging. The server now sends customized IPFIX logs for every connection it makes.

Showing IPFIX statistics

Use these `tmsh` commands to show IPFIX statistics.

1. Access the `tmsh` command-line utility.
2. To show IPFIX usage per IPFIX::destination, use the `show` command on the `sys ipfix destinations tmsh` component:

   ```
   show sys ipfix destination [<destination-name>]
   ```

   Note: *The optional <destination-name> narrows the focus to a single IPFIX::destination. If you omit this, the output shows statistics for all active IPFIX destinations.*

   For example, this shows statistics for two IPFIX destinations:

```
root@(localhost)(cfg-sync Standalone)(Active)(/Common)(tmos)# show sys ipfix
 destination

-------------------------------------------
Sys::IPFIX Destination: ipfix_dest_tcp_14279
-------------------------------------------
Templates
  Registered            4
  Failed                0
  Withdrawn             2
  Timed Out             2
  Expired               2
  PDUs Sent             0
  PDUs Rejected         0

Data
  Records Added        15
  Records Failed        0
  PDUs Queued           2
  PDUs Rejected        13
  PDUs Sequenced        0

Connections Setup       0
Connections Closed      0
Queue High-Water Mark   0

-------------------------------------------
Sys::IPFIX Destination: ipfix_dest_udp_14279
-------------------------------------------
Templates
  Registered           0
  Failed               0
  Withdrawn            0
  Timed Out            0
  Expired              0
  PDUs Sent            0
  PDUs Rejected        0

Data
  Records Added        0
  Records Failed       0
  PDUs Queued          0
  PDUs Rejected        0
  PDUs Sequenced       0

Connections Setup      0
Connections Closed     0
Queue High-Water Mark  0
```

```
root@(localhost)(cfg-sync Standalone)(Active)(/Common)(tmos)#
```

3. To show IPFIX-iRule usage on various TMM cores, use the `show` command on the `sys ipfix rules` `tmsh` component:

   ```
   show sys ipfix rules
   ```

   Each TMM core appears in its own table. The columns indicate the numbers of iRule objects created:

   - The **Template** column shows the number of times that an iRule invoked the `IPFIX::template create` command.
   - The **Message** column corresponds to the `IPFIX::message create` command.
   - The **Destination** column corresponds to the `IPFIX::destination create` command.

   The **Total Sends** field shows the total number of `IPFIX:message send` commands invoked on this core, and the **Send Failures** field shows how many of them failed.

   For example:

```
root@(localhost)(cfg-sync Standalone)(Active)(/Common)(tmos)# show sys ipfix
 irules

-------------------------------------------
Sys::TMM IPFIX iRules: 0.0
-------------------------------------------
Memory         Template  Message  Destination
  Allocation          1        7            1
  Outstanding         1        0            1

Total Sends           7
Send Failures         0

-------------------------------------------
Sys::TMM IPFIX iRules: 0.1
-------------------------------------------
Memory         Template  Message  Destination
  Allocation          1        8            1
  Outstanding         1        0            1

Total Sends           8
Send Failures         0

root@(localhost)(cfg-sync Standalone)(Active)(/Common)(tmos)#
```

Advanced IPFIX iRule tasks

Creating customized IPFIX elements

IPFIX is a logging protocol that defines templates for each log message. Each template contains one or more IPFIX elements (also known as Information Elements [IEs]) in a specific order. Many IPFIX elements are defined by IANA; you can use the following steps to define your own.

1. Access the `tmsh` command-line utility.
2. Use the `create` command on the **sys ipfix element** tmsh component:

```
create sys ipfix element <name> id <number> data-type <type> [size <bytes>]
enterprise-id <number>
```

- **element <name>** can be a unique name or the name of an existing IANA element. If it is an IANA-defined name, it currently exists with a ":base" extension at the end of its name; you can redefine it by entering the same name without the ":base" at the end, and entering an **enterprise-id** of zero. Your definition takes precedence over the "base" definition from IANA.
- **id <number>** must be in the range 1-32767.
- **data-type <type>** is a data-type defined by IANA. Type **<Tab>** for a complete list of valid choices.
- **size <bytes>** is only valid with a **data-type** of string or octarray. A size of zero (the default) indicates a variable, unbounded length. Variable length fields cannot function with NetFlow v9 collectors.
- **enterprise-id <number>** identifies the company that owns this IPFIX element. If you enter zero, you are defining or redefining an IANA element; the definition you enter takes precedence over the base definition from IANA.

For example, these commands create elements for an HTTP request:

```
create sys ipfix element flowStartSeconds id 1 data-type dateTimeSeconds
enterprise-id 65
create sys ipfix element httpPath id 2 data-type string size 128 enterprise-id
 65
create sys ipfix element httpMethod id 3 data-type string size 128
enterprise-id 65
create sys ipfix element httpUserAgent id 4 data-type string enterprise-id
65
```

3. To edit an IPFIX element, use the `modify` command on the **sys ipfix element** `tmsh` component:

   ```
   modify sys ipfix element <name> [id <number>] [data-type <type>] [size <bytes>]
   [enterprise-id <number>]
   ```

   The element name is required, but you only need to enter the options that you are modifying after that. The options details are the same as for the `create` command.

   Note: *You cannot modify a base IANA element, with `":base"` at the end of its name.*

   For example, this command modifies the `httpPath element` to have a variable length (a zero setting makes the length variable):

   ```
   modify sys ipfix element httpPath size 0
   ```

4. To delete an IPFIX element, use the `delete` command on the `sys ipfix element` `tmsh` component:

   ```
   delete sys ipfix element <name>+
   ```

   At least one element name is required, and you can enter multiple element names.

   Note: *You cannot delete a base IANA element, with `":base"` at the end of its name.*

   For example, this command removes the `httpUserAgent element`:

   ```
   delete sys ipfix element httpUserAgent
   ```

5. To list all IPFIX elements, including IANA-defined elements and elements created this way, use the `list` command on the `sys ipfix element` `tmsh` component:

   ```
   list sys ipfix element <name>
   ```

The element name is only required if you want to list a single element. Without this option, the command lists all of them.

For example, this command lists the `httpPath` component:

```
root@(localhost)(cfg-sync Standalone)(Active)(/Common)(tmos.sys)# list sys
ipfix element httpPath
sys ipfix element httpPath {
    data-type string
    enterprise-id 65
    id 2
}
root@(localhost)(cfg-sync Standalone)(Active)(/Common)(tmos.sys)#
```

The element name has a `":base"` extension for elements that are defined by IANA. If you redefined an IANA element, it appears separately without the `":base"` extension.

This example shows the IPFIX elements whose names start with `flowStartSeconds`. The result displays the user-defined version of that element together with the base version:

```
root@(localhost)(cfg-sync Standalone)(Active)(/Common)(tmos)# list sys ipfix
 element flowStartSeconds*
sys ipfix element flowStartSeconds {
    data-type dateTimeSeconds
    enterprise-id 65
    id 1
    size 128
}
sys ipfix element flowStartSeconds:base {
    data-type dateTimeSeconds
    enterprise-id 0
    id 150
}
root@(localhost)(cfg-sync Standalone)(Active)(/Common)(tmos)
```

You can use these custom elements in any iRule that creates IPFIX logs.

Cleaning up memory in an IPFIX iRule

You can create an iRule that reads IP packets and logs information about them to your IPFIX collectors. You can also use certain iRules® commands to clean up memory reserved for unused IPFIX components. These cleanup commands are rarely necessary, since memory cleanup occurs after each iRule finishes processing on a given connection. They are designed for long-running iRules with multiple messages, templates, and destinations.

1. On the Main tab, click **Local Traffic** > **iRules**.
   The iRule List screen displays a list of existing iRules®.
2. Click on the name of any existing iRule that you would like to edit.
   The iRule screen opens.
3. In the **Definition** field, edit the iRule with any of the following memory-cleanup commands, as needed:
   a) To free up memory after an IPFIX message is sent, or to delete the message before sending it, use the following syntax:
      `IPFIX::msg delete <ipfix_message_handle>`
   b) After you have finished using an IPFIX::template, you can remove it with the following syntax:
      `IPFIX::template delete <ipfix_dest_handle> <ipfix_template_handle>`

The <ipfix_dest_handle> is required so that the BIG-IP system can send IPFIX template-withdrawal messages to the destination's IPFIX collectors. The system then deletes the <ipfix_template_handle> from memory.

This prevents sending any further IPFIX logs that use this template.

c) After you have finished using an IPFIX::destination, you can close it with the following syntax:

```
IPFIX::destination close <ipfix_dest_handle>
```

This prevents sending any further IPFIX logs to the destination. Use `IPFIX::destination open` to reopen the same log publisher as an IPFIX destination.

4. Click **Finished**.

Implementation result

Now you have an implementation in which the BIG-IP® system logs messages about network events and sends the log messages to a pool of IPFIX collectors.

Monitoring BIG-IP System Traffic with SNMP

Overview: Configuring network monitoring using SNMP

SNMP is an industry standard protocol for monitoring devices on IP networks. You can configure the BIG-IP® system with SNMP traps and an SNMP agent that sends data to an SNMP manager. You can then use the collected data to help you troubleshoot the BIG-IP system.

SNMP deployment worksheet

This table provides information about the prerequisites for a BIG-IP® system SNMP deployment.

Configuration component	Prerequisite tasks and considerations
SNMP administrator contact information	Determine who is responsible for SNMP administration for the BIG-IP system. The contact information is a MIB-II simple string variable.
Machine location	Determine the location of the BIG-IP system. The contact information is a MIB-II simple string variable.
BIG-IP system user role	Ensure that your assigned user role is either Administrator or Resource Administrator.
BIG-IP system client allow list	Gather the IP or network addresses (with netmask) of the SNMP managers from which the SNMP agent will accept requests.
SNMP manager routes	Define a route to the BIG-IP system on the SNMP manager to specify where the manager sends SNMP requests. If the SNMP manager is not on the same subnet as the BIG-IP system, you must also add the route to the SNMP manager to the BIG-IP system routes table, and enable one of the dynamic routing protocols. ***Note:*** *For VIPRION systems, the route you define to the BIG-IP system on the SNMP manager must be the route to the VIPRION system cluster management IP address, because SNMP traps are sourced from that IP address.*
Access	Determine the OID for the top-most node of the SNMP tree to which the access applies.
Communities	Determine the v1 and v2c communities and the IP addresses of the SNMP managers that you want to grant access to SNMP data.
Users	Determine the v3 users that you want to grant access to SNMP data. Gather authentication types and passwords, and privacy protocols and passwords for each user.
BIG-IP system statistics	BIG-IP system statistics are defined by 64-bit counters. SNMP v2c and v3 support 64-bit counters. Therefore, your SNMP manager must use SNMP v2c or v3 to query the BIG-IP system. SNMP v1 does not support 64-bit counters.

Component overview

SNMP device management is based on the standard MIB-II, as well as object IDs and MIB files. A standard SNMP implementation, includes the following components:

SNMP manager
The part of an SNMP system that runs on a management system and makes requests to the BIG-IP system.

SNMP agent
The part of an SNMP system that runs on the BIG-IP system and fulfills requests from the SNMP manager.

Management Information Base (MIB)
A set of data that defines the standard objects on the BIG-IP system that can be managed by the SNMP manager. The objects are presented in a hierarchical, tree structure.

Object identifier (OID)
A numeric identifier that indicates the location of an object within the MIB tree. Each object defined in the MIB has a unique OID, written as a series of integers.

Enterprise MIB
A set of data that defines the objects on the BIG-IP system that are specific to F5 Networks, Inc., and can be managed by the SNMP manager.

MIB file
An ASCII text file that describes SNMP network elements as a list of data objects, including the data type and current validity of each object, as well as a brief description of the purpose of each object. A set of MIB files consists of standard SNMP MIB files and enterprise MIB files.

Permissions on SNMP data objects

This table shows that access to an object depends on the object's access type and the access assigned to a user.

Access type	Assigned access level (for community or user)	Result access
Read-only	Read-only	Read-only
Read-only	Read-write	Read-only
Read-write	Read-only	Read-only
Read-write	Read-write	Read-write

About enterprise MIB files

The enterprise MIB files contain F5 Networks specific information. All OIDS for the BIG-IP® system data are contained in the F5 enterprise MIB files, including all interface statistics (**1.3.6.1.4.1.3375.2.1.2.4** (**sysNetwork.sysInterfaces**)). These enterprise MIB files reside on the BIG-IP system:

F5-BIGIP-COMMON-MIB.txt
Contains information that the SNMP manager can use to help manage F5-specific notifications (SNMP traps) that all other BIG-IP MIB files reference.

F5-BIGIP-SYSTEM-MIB.txt
Contains information that the SNMP manager can use to help manage BIG-IP system objects, such as global statistic data, network information, and platform information.

F5-BIGIP-LOCAL-MIB.txt
Contains information that the SNMP manager can use to help manage BIG-IP local traffic objects, such as virtual servers, pools, nodes, profiles, health monitors, iRules®, and SNATs.

F5-BIGIP-GLOBAL-MIB.txt
Contains information that the SNMP manager can use to help manage global traffic objects, such as wide IPs, virtual servers, pools, links, servers, and data centers.

F5-BIGIP-APM-MIB.txt
Contains information that the SNMP manager can use to help manage access policy objects, such as profiles, statistics, lease pools, and ACLs.

F5-BIGIP-WAM-MIB.txt
Contains information that the SNMP manager can use to help manage traffic acceleration objects, such as applications, profiles, and statistics.

Task summary

Perform these tasks when working with MIB files.

Downloading enterprise and NET-SNMP MIBs to the SNMP manager
Viewing objects in enterprise MIB files
Viewing SNMP traps in F5-BIGIP-COMMON-MIB.txt
Viewing dynamic routing SNMP traps and associated OIDs
Monitoring BIG-IP system processes using SNMP
Collecting BIG-IP system memory usage data using SNMP
Collecting BIG-IP system data on HTTP requests using SNMP
Collecting BIG-IP system data on throughput rates using SNMP
Collecting BIG-IP system data on RAM cache using SNMP
Collecting BIG-IP system data on SSL transactions using SNMP
Collecting BIG-IP system data on CPU usage based on a predefined polling interval
Collecting BIG-IP system data on CPU usage based on a custom polling interval
Collecting BIG-IP system performance data on new connections using SNMP
Collecting BIG-IP system performance data on active connections using SNMP

Downloading enterprise and NET-SNMP MIBs to the SNMP manager

View the set of standard SNMP MIB files that you can download to the SNMP manager, by listing the contents of the BIG-IP® system directory `/usr/share/snmp/mibs`.

Download compressed files that contain the enterprise and NET-SNMP MIBs.

1. Click the **About** tab.
2. Click **Downloads**.
3. Click **Download F5 MIBs (mibs_f5.tar.gz)** or **Download NET-SNMP MIBs (mibs_netsnmp.tar.gz)**.
4. Follow the instructions on the screen to complete the download.

Viewing objects in enterprise MIB files

You must have the `Administrator` user role assigned to your user account.

View information about a BIG-IP system object by listing the contents of an enterprise MIB file.

1. Access a console window on the BIG-IP system.
2. At the command prompt, list the contents of the directory `/usr/share/snmp/mibs`.
3. View available objects in the relevant MIB file.

Viewing SNMP traps in F5-BIGIP-COMMON-MIB.txt

Verify that you have the `Administrator` user role assigned to your user account.

When an F5-specific trap sends a notification to the SNMP manager, the SNMP manager receives a text message describing the event or problem that has occurred. You can identify the traps specified in the F5-BIGIP-COMMON-MIB.txt file by viewing the file.

1. Access a console window on the BIG-IP system.
2. At the command prompt, list the contents of the directory `/usr/share/snmp/mibs`.
3. View the F5-BIGIP-COMMON-MIB.txt file. Look for object names with the designation NOTIFICATION-TYPE.

Viewing dynamic routing SNMP traps and associated OIDs

Verify that you have the `Administrator` user role assigned to your user account.

When you want to set up your network management systems to watch for problems with dynamic routing, you can view SNMP MIB files to discover the SNMP traps that the dynamic routing protocols send, and to find the OIDs that are associated with those traps.

1. Access a console window on the BIG-IP system.
2. At the command prompt, list the contents of the directory `/usr/share/snmp/mibs`.
3. View the following dynamic routing MIB files:
   - BGP4-MIB.txt
   - ISIS-MIB.txt
   - OSPF6-MIB.txt
   - OSPF-MIB.txt
   - OSPF-TRAP-MIB.txt
   - RIPv2-MIB.txt

Monitoring BIG-IP system processes using SNMP

Ensure that your SNMP manager is running either SNMP v2c or SNMP v3, because all BIG-IP® system statistics are defined by 64-bit counters, and only SNMP v2c and SNMP v3 support 64-bit counters. Ensure that you have downloaded the F-5 Networks enterprise and NET-SNMP MIBs to the SNMP manager.

You can monitor a specific process on the BIG-IP system using SNMP. To do this you can use the HOST-RESOURCES MIB and write a script to monitor the process.

Write a script to monitor a BIG-IP system process using the HOST-RESOURCES MIB.

For example, this command determines the number of TMM processes currently running on the system: `snmpwalk -v2c -c public localhost hrSWRunName | egrep "\"tmm(.[0-9]+)?\"" | wc -l`

The script can now query the BIG-IP system about the status of processes.

Collecting BIG-IP system memory usage data using SNMP

You can use an SNMP command with OIDs to gather data on the number of bytes of memory currently being used on the BIG-IP® system.

Note: *To interpret data on memory use, you do not need to perform a calculation on the collected data.*

Write an SNMP command to gather data on the number of bytes of memory currently being used on the BIG-IP system.

For example, this SNMP command collects data on current memory usage, where `public` is the community name and `bigip` is the host name of the BIG-IP system: `snmpget -c public bigip sysGlobalStat.sysStatMemoryUsed.0`

The SNMP manager can now query the BIG-IP system about CPU and memory usage.

Collecting BIG-IP system data on HTTP requests using SNMP

You can use SNMP commands with an OID to gather and interpret data on the number of current HTTP requests on the BIG-IP® system. The following table shows the required OIDs for polling data on HTTP requests.

Performance Graph	Graph Metrics	Required SNMP OIDs
HTTP Requests	HTTP Requests	sysStatHttpRequests (.1.3.6.1.4.1.3375.2.1.1.2.1.56)

The following table shows the required calculations for interpreting metrics on HTTP requests.

Performance Graph	Graph Metric	Required calculations for HTTP requests
HTTP Requests	HTTP Requests	<DeltaStatHttpRequests> / <interval>

1. For each OID, perform two separate pools, at an interval of your choice. For example, poll OID `sysStatHttpRequests (.1.3.6.1.4.1.3375.2.1.1.2.1.56)` twice, at a 10-second interval. This results in two values, `<sysStatHttpRequests1>` and `<sysStatHttpRequests2>`.

2. Calculate the delta of the two poll values. For example:

```
<DeltaStatHttpRequests> = <sysStatHttpRequests2> - <sysStatHttpRequests1>
```

3. Perform the calculation on the OID deltas. The value for *interval* is 10. For example, to calculate the value of the HTTP Requests graph metric:

```
(<DeltaStatHttpRequests>) / <interval>
```

Collecting BIG-IP system data on throughput rates using SNMP

You can use SNMP commands with various OIDs to gather and interpret data on the throughput rate on the BIG-IP® system. The following table shows the individual OIDs that you must poll, retrieving two separate poll values for each OID.

Performance Graph	Graph Metrics	Required SNMP OIDs
Throughput (summary graph)	Client Bits Client Bits Server Bits Server Bits	sysStatClientBytesIn (.1.3.6.1.4.1.3375.2.1.1.2.1.3) sysStatClientBytesOut (.1.3.6.1.4.1.3375.2.1.1.2.1.5) sysStatServerBytesIn (.1.3.6.1.4.1.3375.2.1.1.2.1.10) sysStatServerBytesOut (.1.3.6.1.4.1.3375.2.1.1.2.1.12)
Client-side Throughput (detailed graph)	Client Bits In Client Bits Out	sysStatClientBytesIn (.1.3.6.1.4.1.3375.2.1.1.2.1.3) sysStatClientBytesOut (.1.3.6.1.4.1.3375.2.1.1.2.1.5)
Server-side Throughput (detailed graph)	Server Bits In Server Bits Out	sysStatServerBytesIn (.1.3.6.1.4.1.3375.2.1.1.2.1.10) sysStatServerBytesOut (.1.3.6.1.4.1.3375.2.1.1.2.1.12)
HTTP Compression Rate (detailed graph)	Compression	sysHttpCompressionStatPrecompressBytes (.1.3.6.1.4.1.3375.2.1.1.2.22.2)

The following table shows the required calculations for interpreting metrics on throughput rates.

Performance Graph	Graph Metrics	Required calculations for throughput rates
Throughput (summary graph)	Client Bits Server Bits Compression	((<DeltaStatClientBytesIn> + <DeltasysStatClientBytesOut>)*8 / <interval> ((<DeltaStatServerBytesIn> + <DeltaServersslStatServerBytesOut>)*8 / <interval> (<DeltaHttpStatPrecompressBytes>)*8 / <interval>
Throughput (detailed graph)	Client Bits In Client Bits Out Server Bits In Server Bits Out Compression	(<DeltaStatClientBytesIn>)*8 / <interval> (<DeltaStatClientBytesOut>*8) / <interval> (<DeltaStatServerBytesIn >*8) / <interval> (<DeltaStatServerBytesOut>*8) / <interval> (<DeltaHttpStatPrecompressBytes>*8) / <interval>

1. For each OID, perform two separate pools, at an interval of your choice. For example, poll OID `sysStatServerBytesIn (.1.3.6.1.4.1.3375.2.1.1.2.1.10)` twice, at a 10-second interval. This results in two values, `<sysStatServerBytesIn1>` and `<sysStatServerBytesIn2>`.
2. Calculate the delta of the two poll values. For example, for the Server Bits In graphic metric, perform this calculation:

```
<DeltaStatServerBytesIn> = <sysStatServerBytesIn2> - <sysStatServerBytesIn1>
```

3. Perform the calculation on the OID deltas. The value for *interval* is 10. For example, to calculate the value of the Server Bits In graph metric:

```
(<DeltaStatServerBytesIn>) / <interval>
```

Collecting BIG-IP system data on RAM cache using SNMP

You can use an SNMP command with various OIDs to gather and interpret data on RAM cache use. The following table shows the required OIDs for polling for data on RAM Cache use.

Performance Graph	Graph Metric	Required SNMP OIDs
RAM Cache Utilization	Hit Rate	sysWebAccelerationStatCacheHits (.1.3.6.1.4.1.3375.2.1.1.2.23.2) sysWebAccelerationStatCacheMisses (.1.3.6.1.4.1.3375.2.1.1.2.23.3)
CPU Cache Utilization	Byte Rate	sysWebAccelerationStatCacheHitBytes (.1.3.6.1.4.1.3375.2.1.1.2.23.5) sysWebAccelerationStatCacheMissBytes (.1.3.6.1.4.1.3375.2.1.1.2.23.6)
RAM Cache Utilization	Eviction Rate	sysWebAccelerationStatCacheEvictions (.1.3.6.1.4.1.3375.2.1.1.2.23.10), sysWebAccelerationStatCacheHits (.1.3.6.1.4.1.3375.2.1.1.2.23.2) sysWebAccelerationStatCacheMisses (.1.3.6.1.4.1.3375.2.1.1.2.23.3)

The following table shows the required calculations for interpreting metrics on RAM Cache use.

Performance Graph	Graph Metric	Required SNMP OIDs
RAM cache Utilization	Hit Rate	<sysWebAccelerationStatCacheHits1>) / (<sysWebAccelerationStatCacheHits1> + <sysWebAccelerationStatCacheMisses1>) / *100
RAM cache Utilization	Byte Rate	<sysWebAccelerationStatCacheHitBytes1) / (<sysWebAccelerationStatCacheHitBytes1> + <sysWebAccelerationStatCacheMissBytes1>) / *100
RAM cache Utilization	Eviction Rate	<sysWebAccelerationStatCacheEvictions1>) / (<sysWebAccelerationStatCacheHits1> + <sysWebAccelerationStatCacheMisses1>) / *100

1. For each OID, poll for data. For example, poll OID `sysWebAccelerationStatCacheHits(.1.3.6.1.4.1.3375.2.1.1.2.23.2)`. This results in a value `<sysWebAccelerationStatCacheHits>` .
2. Poll OID `sysWebAccelerationStatCacheHits(.1.3.6.1.4.1.3375.2.1.1.2.23.2)`. This results in a value `<sysWebAccelerationStatCacheMisses>`.

3. Perform the calculation using the OID data. For example, to calculate the value of the Hit Rate graphic metric:

```
<sysWebAccelerationStatCacheHits> / <sysWebAccelerationStatCacheHits1> + <>)
 *100).
```

Collecting BIG-IP system data on SSL transactions using SNMP

You can use SNMP commands with an OID to gather and interpret data on SSL performance. The following table shows the individual OIDS that you must use to poll for SSL transactions using SNMP.

Performance Graph	Graph Metrics	Required SNMP OIDs
SSL TPS	SSL TPS	sysClientsslStatToNativeConns (.1.3.6.1.4.1.3375.2.1.1.2.9.6)
SSL TPS	SSL TPS	sysClientsslStatTotCompatConns (.1.3.6.1.4.1.3375.2.1.1.2.9.9)
SSL TPS	SSL TPS	sysServersslStatTotNativeConns (.1.3.6.1.4.1.3375.2.1.1.2.10.6)
SSL TPS	SSL TPS	sysServersslStatTotCompatConns (.1.3.6.1.4.1.3375.2.1.1.2.10.9)

The following table shows the required calculations for interpreting metrics on SSL transactions using SNMP.

Performance Graph	Graph Metric	Required calculations for SSL TPS
SSL TPS	SSL TPS	<DeltaClientsslStatClientTotConns>) / (<interval>

1. For each OID, poll for data. For example, poll OID `sysClientsslStatToNativeConns (.1.3.6.1.4.1.3375.2.1.1.2.23.2)` and `sysClientsslStatTotCompatConns (.1.3.6.1.4.1.3375.2.1.1.2.9.9)`.
2. Add the two values together. This results in the value `sysClientsslStartTotConns1`.
3. Poll the two OIDs again, within ten seconds of the previous polls.
4. Again, add the two values together. This results in the value `sysClientsslStatToComms2`.
5. Calculate the delta of the two sums:

```
<DeltaClientsslStatTotConns> = <sysClientsslStatTotConns2> -
<sysClientsslStatTotConns1>.
```

6. Perform the calculation on the OID deltas. The value for interval is 10. For example, to calculate the value of the SSL transactions using SNMP:

```
(<DeltaClientsslStatClientTotConns>) / <interval>
```

Collecting BIG-IP system data on CPU usage based on a predefined polling interval

For the CPU[0-n] and Global Host CPU Usage graph metrics, you can instruct the BIG-IP® system to gather and collect CPU usage data automatically, based on a predifined polling interval. Use the sysMultiHostCpu and sysGlobalHostCpu MIBs.

The following table shows the required OIDs for automatic collection of CPU[0-n] graphic metrics.

Performance Graph	Graph Metric	Required SNMP OIDs
CPU Usage	CPU[0-n]	**5-second Polling Interval** sysMultiHostCpuUser5s (.1.3.6.1.4.1.3375.2.1.7.5.2.1.12) sysMultiHostCpuNice5s (.1.3.6.1.4.1.3375.2.1.7.5.2.1.13) sysMultiHostCpuSystem5s (.1.3.6.1.4.1.3375.2.1.7.5.2.1.14) sysMultiHostCpuIdle5s (.1.3.6.1.4.1.3375.2.1.7.5.2.1.15) sysMultiHostCpuIrq5s (.1.3.6.1.4.1.3375.2.1.7.5.2.1.16) sysMultiHostCpuSoftirq5s (.1.3.6.1.4.1.3375.2.1.7.5.2.1.17) sysMultiHostCpuIowait5s (.1.3.6.1.4.1.3375.2.1.7.5.2.1.18) sysMultiHostCpuUsageRatio5s (.1.3.6.1.4.1.3375.2.1.7.5.2.1.19) sysMultiHostCpuUsageRatio (.1.3.6.1.4.1.3375.2.1.7.5.2.1.11)
CPU Usage	CPU[0-n]	**1-minute Polling Interval** sysMultiHostCpuUser1m (.1.3.6.1.4.1.3375.2.1.7.5.2.1.20) sysMultiHostCpuNice1m (.1.3.6.1.4.1.3375.2.1.7.5.2.1.21) sysMultiHostCpuSystem1m (.1.3.6.1.4.1.3375.2.1.7.5.2.1.22) sysMultiHostCpuIdle1m (.1.3.6.1.4.1.3375.2.1.7.5.2.1.23) sysMultiHostCpuIrq1m (.1.3.6.1.4.1.3375.2.1.7.5.2.1.24) sysMultiHostCpuSoftirq1m (.1.3.6.1.4.1.3375.2.1.7.5.2.1.25) sysMultiHostCpuIowait1m (.1.3.6.1.4.1.3375.2.1.7.5.2.1.26) sysMultiHostCpuUsageRatio1m (.1.3.6.1.4.1.3375.2.1.7.5.2.1.26)
CPU Usage	CPU[0-n]	**5-minute Polling Interval** sysMultiHostCpuUse5m (.1.3.6.1.4.1.3375.2.1.7.5.2.1.28) sysMultiHostCpuNice5m (.1.3.6.1.4.1.3375.2.1.7.5.2.1.29) sysMultiHostCpuSystem5m (.1.3.6.1.4.1.3375.2.1.7.5.2.1.30) sysMultiHostCpuIdle5m (.1.3.6.1.4.1.3375.2.1.7.5.2.1.31) sysMultiHostCpuIrq5m (.1.3.6.1.4.1.3375.2.1.7.5.2.1.32) sysMultiHostCpuSoftirq5m (.1.3.6.1.4.1.3375.2.1.7.5.2.1.33) sysMultiHostCpuIowait5m (.1.3.6.1.4.1.3375.2.1.7.5.2.1.34) sysMultiHostCpuUsageRatio5m (.1.3.6.1.4.1.3375.2.1.7.5.2.1.35)

The following table shows the required OIDs for automatic collection of Global Host CPU Usage graph metrics.

Performance Graph	Graph Metric	Required SNMP OIDs
CPU Usage	Global Host CPU Usage	**5-second Polling Interval** sysMultiHostCpuUser5s (.1.3.6.1.4.1.3375.2.1.1.2.20.14) sysMultiHostCpuNice5s (.1.3.6.1.4.1.3375.2.1.1.2.20.15) sysMultiHostCpuSystem5s (.1.3.6.1.4.1.3375.2.1.1.2.20.16) sysMultiHostCpuIdle5s (.1.3.6.1.4.1.3375.2.1.1.2.20.17) sysMultiHostCpuIrq5s (.1.3.6.1.4.1.3375.2.1.1.2.20.18) sysMultiHostCpuSoftirq5s (.1.3.6.1.4.1.3375.2.1.1.2.20.19) sysMultiHostCpuIowait5s (.1.3.6.1.4.1.3375.2.1.1.2.20.20)

Performance Graph	Graph Metric	Required SNMP OIDs
		sysMultiHostCpuUsageRatio5s (.1.3.6.1.4.1.3375.2.1.1.2.20.21) sysMultiHostCpuUsageRatio (.1.3.6.1.4.1.3375.2.1.1.2.20.13)
CPU Usage	Global Host CPU Usage	**1-minute Polling Interval** sysMultiHostCpuUser1m (.1.3.6.1.4.1.3375.2.1.1.2.20.22) sysMultiHostCpuNice1m (.1.3.6.1.4.1.3375.2.1.1.2.20.23) sysMultiHostCpuSystem1m (.1.3.6.1.4.1.3375.2.1.1.2.20.24) sysMultiHostCpuIdle1m (.1.3.6.1.4.1.3375.2.1.1.2.20.25) sysMultiHostCpuIrq1m (.1.3.6.1.4.1.3375.2.1.1.2.20.26) sysMultiHostCpuSoftirq1m (.1.3.6.1.4.1.3375.2.1.1.2.20.27) sysMultiHostCpuIowait1m (.1.3.6.1.4.1.3375.2.1.1.2.20.28) sysMultiHostCpuUsageRatio1m (.1.3.6.1.4.1.3375.2.1.1.2.20.29)
CPU Usage	Global Host CPU Usage	**5-minute Polling Interval** sysMultiHostCpuUse5m (.1.3.6.1.4.1.3375.2.1.1.2.20.30) sysMultiHostCpuNice5m (.1.3.6.1.4.1.3375.2.1.1.2.20.31) sysMultiHostCpuSystem5m (.1.3.6.1.4.1.3375.2.1.1.2.20.32) sysMultiHostCpuIdle5m (.1.3.6.1.4.1.3375.2.1.1.2.20.33)) sysMultiHostCpuIrq5m (.1.3.6.1.4.1.3375.2.1.1.2.20.34) sysMultiHostCpuSoftirq5m (.1.3.6.1.4.1.3375.2.1.1.2.20.35) sysMultiHostCpuIowait5m (.1.3.6.1.4.1.3375.2.1.1.2.20.36) sysMultiHostCpuUsageRatio5m (.1.3.6.1.4.1.3375.2.1.1.2.20.37)

Collecting BIG-IP system data on CPU usage based on a custom polling interval

For the CPU[0-n], Global Host CPU, and TMM CPU Usage graph metrics, an alternative to instructing the BIG-IP® system to collect CPU usage data automatically, is to do it maually, based on a custom polling interval. For the CPU[0-n] and Global Host CPU graph metrics, use the sysMultiHostCpu and sysGlobalHostCpu MIBs. For the TMM CPU Usage graphic metric, use the sysStatTm MIB.

The following table shows the required SNMP OIDs for collecting CPU data manually.

Performance Graph	Graph Metric	Required SNMP OIDs
CPU Usage	CPU[0-n]	sysMultiHostCpuUser (.1.3.6.1.4.1.3375.2.1.7.5.2.1.4) sysMultiHostCpuNice (.1.3.6.1.4.1.3375.2.1.7.5.2.1.5) sysMultiHostCpuSystem (.1.3.6.1.4.1.3375.2.1.7.5.2.1.6) sysMultiHostCpuIdle (.1.3.6.1.4.1.3375.2.1.7.5.2.1.7) sysMultiHostCpuIrq (.1.3.6.1.4.1.3375.2.1.7.5.2.1.8) sysMultiHostCpuSoftirq (.1.3.6.1.4.1.3375.2.1.7.5.2.1.9) sysMultiHostCpuIowait (.1.3.6.1.4.1.3375.2.1.7.5.2.1.10)
CPU Usage	Global Host CPU Usage	sysGlobalHostCpuCount (.1.3.6.1.4.1.3375.2.1.1.2.20.4) sysGlobalHostActiveCpu (.1.3.6.1.4.1.3375.2.1.1.2.20.5) sysGlobalHostCpuUser (.1.3.6.1.4.1.3375.2.1.1.2.20.6) sysGlobalHostCpuNice (.1.3.6.1.4.1.3375.2.1.1.2.20.7) sysGlobalHostCpuSystem (.1.3.6.1.4.1.3375.2.1.1.2.20.8) sysGlobalHostCpuIdle (.1.3.6.1.4.1.3375.2.1.1.2.20.9) sysGlobalHostCpuIrq (.1.3.6.1.4.1.3375.2.1.1.2.20.10) sysGlobalHostCpuSoftirq (.1.3.6.1.4.1.3375.2.1.1.2.20.11) sysGlobalHostCpuIowait (.1.3.6.1.4.1.3375.2.1.1.2.20.12)

Performance Graph	Graph Metric	Required SNMP OIDs
CPU Usage	TMM CPU Usage	sysStatTmTotalCycles (.1.3.6.1.4.1.3375.2.1.1.2.1.41) sysStatTmIdleCycles (.1.3.6.1.4.1.3375.2.1.1.2.1.42) sysStatTmSleepCycles (.1.3.6.1.4.1.3375.2.1.1.2.1.43) sysTmmStatTmUsageRatio5s (.1.3.6.1.4.1.3375.2.1.8.2.3.1.37.[tmm_id]) sysTmmStatTmUsageRatio1m (.1.3.6.1.4.1.3375.2.1.8.2.3.1.38.[tmm_id]) sysTmmStatTmUsageRatio5m (.1.3.6.1.4.1.3375.2.1.8.2.3.1.39.[tmm_id])

The following table shows the formulas for calculating metrics on CPU use.

Performance Graph	Graph Metric	Required calculations for CPU use
CPU Usage	CPU[0-n]	(<DeltaCpuUsers>) + (<DeltaCpuNice> + <DeltaCpuSystem> / (<DeltaCpuUsers>) + <DeltaCpuNice> + <DeltaCpuIdle> + <DeltaCpuSystem> + <DeltaCpulrq> + <DeltaCpuSoftirq> + <DeltaCpulowait>) *100
CPU Usage	Global Host CPU Usage	(<DeltaCpuUsers>) + (<DeltaCpuNice> + <DeltaCpuSystem> / (<DeltaCpuUsers>) + <DeltaCpuNice> + <DeltaCpuIdle> + <DeltaCpuSystem> + <DeltaCpulrq> + <DeltaCpuSoftirq> + <DeltaCpulowait>) *100
CPU Usage	TMM CPU Usage	((<DeltaTmTotalCycles>) - (<DeltaTmidleCycles> + <DeltaTmSleepCycles>)) / <DeltaTmTotalCycles>) *100

1. Poll the OID `sysMultiHostCpuUser (.1.3.6.1.4.1.3375.2.1.7.5.2.1.4)` twice, at a 10-second interval. This results in two values, `sysMultiHostCpuUser1and` and `sysMultiHostCpuUser2`.
2. Calculate the delta of the two poll values. For example:

```
<DeltaCpuUser> = <sysMultiHostCpuUser2> - <sysMultiHostCpuUser1>.
```

3. Repeat steps 1 and 2 for each OID pertaining to the **CPU[0-n]** graph metric.
4. Repeat steps 1 and 2 again, using the OIDs from the MIBs **sysStatTm**and **sysGlobalHostCpu**.
5. Calculate the values of the graphic metrics using the formulas in the table above.

Collecting BIG-IP system performance data on new connections using SNMP

You can use SNMP commands with various OIDs to gather and interpret data on the number of new connections on the BIG-IP® system. The following table shows the required OIDs for the Performance graphs in the Configuration utility.

Performance Graph	Graph Metrics	Required SNMP OIDs
New Connections Summary	Client Accepts Server Connects	sysTcpStatAccepts (.1.3.6.1.4.1.3375.2.1.1.2.12.6) sysStatServerTotConns (.1.3.6.1.4.1.3375.2.1.1.2.1.14)
Total New Connections	Client Accepts Server Connects	sysStatClientTotConns(.1.3.6.1.4.1.3375.2.1.1.2.1.7) sysStatServerTotConns (.1.3.6.1.4.1.3375.2.1.1.2.1.14)

Performance Graph	Graph Metrics	Required SNMP OIDs
New Client SSL Profile Connections	SSL Client SSL Server	sysClientsslStatTotNativeConns (.1.3.6.1.4.1.3375.2.1.1.2.9.6), sysClientsslStatTotCompatConns (.1.3.6.1.4.1.3375.2.1.1.2.9.9) sysServersslStatTotNativeConns(.1.3.6.1.4.1.3375.2.1.1.2.10.6), sysServersslStatTotCompatConns (.1.3.6.1.4.1.3375.2.1.1.2.10.9)
New Accepts/ Connects	Client Accepts Server Connects	sysTcpStatAccepts (.1.3.6.1.4.1.3375.2.1.1.2.12.6) sysTcpStatConnects (.1.3.6.1.4.1.3375.2.1.1.2.12.8)

The following table shows the required calculations for interpreting metrics on new connections.

Performance Graph	Graph Metrics	Required SNMP OIDs
New Connections Summary	Client Accepts Server Connects	<DeltaTcpStatAccept> / <interval> <DeltaStatServerTotConns> / <interval>
Total New Connections	Client Connects Server Connects	<DeltaStatClientTotConns> / <interval> <DeltaStatServerTotConns> / <interval>
New Client SSL Profile Connections	SSL Client SSL Server	(<DeltaClientsslStatTotNativeConns> + <DeltaClientsslStatTotCompatConns>) / <interval> (<DeltaServersslStatTotNativeConns> + <DeltaServersslStatTotCompatConns>) / <interval>
New Accepts/ Connects	Client Accepts Server Connects	<DeltaTcpStatAccepts> / <interval> <DeltaTcpStatConnects> / <interval>

1. For each OID, perform two separate polls, at an interval of your choice.

   For example, for the client accepts metric, poll OID `sysTcpStatAccepts (.1.3.6.1.4.1.3375.2.1.1.2.12.6)` twice, at a 10-second interval. This results in two values, `<sysTcpStatAccepts1>` and `<sysTcpStatAccepts2>`.

2. Calculate the delta of the two poll values.

   For example, for the client accepts metric, perform this calculation:

   ```
   <DeltaTcpStatAccepts> = <sysTcpStatAccepts2> - <sysTcpStatAccepts1>
   ```

3. Perform a calculation on the OID deltas. The value for *interval* is the polling interval. For example, to calculate the value of the client accepts metric:

   ```
   <DeltaTcpStatAccepts> / <interval>
   ```

Collecting BIG-IP system performance data on active connections using SNMP

Write an SNMP command with the various OIDs shown in the table to gather and interpret data on the number of active connections on the BIG-IP® system.

Note: *To interpret data on active connections, you do not need to perform any calculations on the collected data.*

Performance Graph	Graph Metrics	Required SNMP OIDs
Active Connections Summary	Connections	sysStatClientCurConns (.1.3.6.1.4.1.3375.2.1.1.2.1.8)
Active Connections Detailed	Client Server SSL Client SSL Server	sysStatClientCurConns (.1.3.6.1.4.1.3375.2.1.1.2.1.8) sysStatServerCurConns (.1.3.6.1.4.1.3375.2.1.1.2.1.15) sysClientsslStatCurConns (.1.3.6.1.4.1.3375.2.1.1.2.9.2) sysServersslStatCurConns (.1.3.6.1.4.1.3375.2.1.1.2.10.2)

About the RMON MIB file

The BIG-IP® system provides the remote network monitoring (RMON) MIB file, RMON-MIB.txt. This file contains remote network monitoring information. The implementation of RMON on the BIG-IP system differs slightly from the standard RMON implementation, in the following ways:

- The BIG-IP system implementation of RMON supports only these four of the nine RMON groups: statistics, history, alarms, and events.
- The RMON-MIB.txt file monitors the BIG-IP system interfaces (that is, sysIfIndex), and not the standard Linux interfaces.
- For hardware reasons, the packet-length-specific statistics in the RMON statistics group offer combined transmission and receiving statistics only. This behavior differs from the behavior described in the definitions of the corresponding OIDs.

About customized MIB entries

Customized MIB entries are defined in a TCL file named `custom_mib.tcl` that you create and save on the BIG-IP® system in the directory `/config/snmp/`. You must register the customized MIB entries and provide callback to the newly registered MIB using the TCL command `register_mib` in this format: `register_mib oid callback type`. The three arguments for the command are described in this table.

Argument	Description
oid	A customized OID with a format of `.1.2.3.4` with a limit of four digits. The common root of a customized MIB OID on the BIG-IP system is `.1.3.6.1.4.1.3375.2.100.`
callback	A TCL procedure that is called when the registered MIB OID is browsed. The procedure cannot have any arguments. The return value of the procedure is returned for the registered MIB entry.
type	The type of MIB entry you are customizing. Four types are supported: INT, STRING, GAUGE, and COUNTER.

Here is sample TCL code for two custom MIBs:

```
register_mib ".1" system_descr string
register_mib ".2" tmmcpucnt int

proc system_descr {}
{
set status [catch {exec uname -a} result]
return $result
}

proc tmmcpucnt {}
{
set status [catch {exec tmctl  cpu_status_stat | grep cpu | wc -l} result]
return $result
}
```

Note: *Customized MIB entries are read-only through SNMP.*

Task summary

Perform this task to create a custom MIB entry.

Creating custom MIB entries

You can add customized MIB entries to a BIG-IP® system to provide visibility to statistics and information that are not available through standard MIBs. These statistics and information can help you make decisions about optimizing the BIG-IP system configuration.

1. Create a TCL file named `custom_mib.tcl` that contains the customized MIB entries you want to use on the BIG-IP system.

   Ensure accuracy of the TCL procedures you use in the file. Avoid errors, such as infinite loops, which can affect how `snmpd` works.

   Note: *`snmpd` restarts after being unresponsive for longer than the heartbeat time interval configured in `config/snmp/bigipTrafficMgmt.conf`.*

2. Save the TCL file to the `/config/snmp/` directory on the BIG-IP system.

   Note: *After you save `custom_mib.tcl`, you can modify the file at any time; however, your changes become effective only after you restart `snmpd`.*

3. Restart `snmpd`.
   Customized MIB entries are registered. If logging is turned on, you might see log entries in `/var/log/snmpd.log`, such as `custom mib initialization completed. total 4 custom mib entry registered.`

Use a MIB browser or `snmpwalk` to obtain the values of the newly registered MIB entries. Use this information to help you manage your network traffic.

Overview: BIG-IP SNMP agent configuration

You can use the industry-standard SNMP protocol to manage BIG-IP® devices on a network. To do this, you must configure the SNMP agent on the BIG-IP system. The primary tasks in configuring the SNMP agent are configuring client access to the SNMP agent, and controlling access to SNMP data.

Task summary

Perform these tasks to configure SNMP on the BIG-IP system.

Specifying SNMP administrator contact information and system location information
Configuring SNMP manager access to the SNMP agent on the BIG-IP system
Granting community access to v1 or v2c SNMP data
Granting user access to v3 SNMP data

Specifying SNMP administrator contact information and system location information

Specify contact information for the SNMP administrator, as well as the physical location of the BIG-IP system running an SNMP agent.

1. On the Main tab, click **System** > **SNMP** > **Agent** > **Configuration**.
2. In the Global Setup area, in the **Contact Information** field, type contact information for the SNMP administrator for this BIG-IP system.

   The contact information is a MIB-II simple string variable. The contact information usually includes both a user name and an email address.
3. In the **Machine Location** field, type the location of the system, such as `Network Closet 1`.

   The machine location is a MIB-II simple string variable.
4. Click **Update**.

Configuring SNMP manager access to the SNMP agent on the BIG-IP system

Gather the IP addresses of the SNMP managers that you want to have access to the SNMP agent on this BIG-IP® system.

Configure the SNMP agent on the BIG-IP system to allow a client running the SNMP manager to access the SNMP agent for the purpose of remotely managing the BIG-IP system.

1. On the Main tab, click **System** > **SNMP** > **Agent** > **Configuration**.
2. In the **Client Allow List** area, for the **Type** setting, select either **Host** or **Network**, depending on whether the IP address you specify is a host system or a subnet.

   Note: *By default, SNMP is enabled only for the BIG-IP system loopback interface (127.0.0.1).*
3. In the **Address** field, type either an IP address or network address from which the SNMP agent can accept requests.
4. If you selected **Network** in step 2, type the netmask in the **Mask** field.
5. Click **Add**.
6. Click **Update**.

The BIG-IP system now contains a list of IP addresses for SNMP managers from which SNMP requests are accepted.

Granting community access to v1 or v2c SNMP data

To better control access to SNMP data, you can assign an access level to an SNMP v1 or v2c community.

Note: *SNMPv1 does not support Counter64 OIDs, which are used for accessing most statistics. Therefore, for SNMPv1 clients, an* `snmp walk` *command skips any OIDs of type Counter64. F5 Networks recommends that you use only clients that support SNMPv2 or higher.*

1. On the Main tab, click **System** > **SNMP** > **Agent** > **Access (v1, v2c)**.
2. Click **Create**.
3. From the **Type** list, select either **IPv4** or **IPv6**.
4. In the **Community** field, type the name of the SNMP community for which you are assigning an access level.
5. From the **Source** list, select **All**, or select **Select** and type the source IP address in the field that displays.
6. In the **OID** field, type the OID for the top-most node of the SNMP tree to which the access applies.
7. From the **Access** list, select an access level, either **Read Only** or **Read/Write**.

   Note: *When you set the access level of a community or user to read/write, and an individual data object has a read-only access type, access to the object remains read-only. In short, the access level or type that is the most secure takes precedence when there is a conflict.*
8. Click **Finished**.

The BIG-IP system updates the `snmpd.conf` file, assigning only a single access setting to the community as shown in this sample `snmpd.conf` file.

Example snmpd.conf file

In the following sample code from an `snmpd.conf` file, string `rocommunity public default` identifies a community named public that has the default read-only access-level. This access-level prevents any allowed SNMP manager in community public from modifying a data object, even if the object has an access type of read/write. The string `rwcommunity public1` identifies a community named public1 as having a read/write access-level. This access-level allows any allowed SNMP manager in community public1 to modify a data object under the tree node `.1.3.6.1.4.1.3375.2.2.10.1` (ltmVirtualServ) on the local host `127.0.0.1`, if that data object has an access type of read/write.

```
rocommunity public default
rwcommunity public1 127.0.0.1  .1.3.6.1.4.1.3375.2.2.10.1
```

Granting user access to v3 SNMP data

To better control access to SNMP data, you can assign an access level to an SNMP v3 user.

1. On the Main tab, click **System** > **SNMP** > **Agent** > **Access (v3)**.
2. Click **Create**.
3. In the **User Name** field, type the name of the user for which you are assigning an access level.
4. In the Authentication area, from the **Type** list, select a type of authentication to use, and then type and confirm the user's password.
5. In the Privacy area, from the **Protocol** list, select a privacy protocol, and either type and confirm the user's password, or select the **Use Authentication Password** check box.
6. In the **OID** field, type the OID for the top-most node of the SNMP tree to which the access applies.
7. From the **Access** list, select an access level, either **Read Only** or **Read/Write**.

   Note: *When you set the access level of a community or user to read/write, and an individual data object has a read-only access type, access to the object remains read-only. In short, the access level or type that is the most secure takes precedence when there is a conflict.*

8. Click **Finished**.

The BIG-IP system updates the `snmpd.conf` file, assigning only a single access setting to the user.

Overview: SNMP trap configuration

SNMP *traps* are definitions of unsolicited notification messages that the BIG-IP® alert system and the SNMP agent send to the SNMP manager when certain events occur on the BIG-IP system. Configuring SNMP traps on a BIG-IP system means configuring how the BIG-IP system handles traps, as well as setting the destination to which the notifications are sent.

The BIG-IP system stores SNMP traps in two specific files:

`/etc/alertd/alert.conf`
Contains default SNMP traps.

Important: *Do not add or remove traps from the `/etc/alertd/alert.conf` file.*

`/config/user_alert.conf`
Contains user-defined SNMP traps.

Task summary

Perform these tasks to configure SNMP traps for certain events and set trap destinations.

Enabling traps for specific events
Setting v1 and v2c trap destinations
Setting v3 trap destinations
Viewing pre-configured SNMP traps
Creating custom SNMP traps

Enabling traps for specific events

You can configure the SNMP agent on the BIG-IP® system to send, or refrain from sending, notifications to the traps destinations.

1. On the Main tab, click **System** > **SNMP** > **Traps** > **Configuration**.
2. To send traps when an administrator starts or stops the SNMP agent, verify that the **Enabled** check box for the **Agent Start/Stop** setting is selected.
3. To send notifications when authentication warnings occur, select the **Enabled** check box for the **Agent Authentication** setting.
4. To send notifications when certain warnings occur, verify that the **Enabled** check box for the **Device** setting is selected.
5. Click **Update**.

The BIG-IP system automatically updates the `alert.conf` file.

Setting v1 and v2c trap destinations

Specify the IP address of the SNMP manager in order for the BIG-IP® system to send notifications.

1. On the Main tab, click **System** > **SNMP** > **Traps** > **Destination**.
2. Click **Create**.
3. For the **Version** setting, select either `v1` or `v2c`.
4. In the **Community** field, type the community name for the SNMP agent running on the BIG-IP system.
5. In the **Destination** field, type the IP address of the SNMP manager.
6. In the **Port** field, type the port number on the SNMP manager that is assigned to receive the traps.
7. Click **Finished**.

Setting v3 trap destinations

Specify the destination SNMP manager to which the BIG-IP® system sends notifications.

1. On the Main tab, click **System** > **SNMP** > **Traps** > **Destination**.
2. Click **Create**.
3. For the **Version** setting, select `v3`.
4. In the **Destination** field, type the IP address of the SNMP manager.
5. In the **Port** field, type the port number on the SNMP manager that is assigned to receive the traps.
6. From the **Security Level** list, select the level of security at which you want SNMP messages processed.

Option	Description
Auth, No Privacy	Process SNMP messages using authentication but without encryption. When you use this value, you must also provide values for the **Security Name**, **Authentication Protocol**, and **Authentication Password** settings.
Auth and Privacy	Process SNMP messages using authentication and encryption. When you use this value, you must also provide values for the **Security Name**, **Authentication Protocol**, **Authentication Password**, **Privacy Protocol**, and **Privacy Password** settings.

7. In the **Security Name** field, type the user name the system uses to handle SNMP v3 traps.
8. In the **Engine ID** field, type an administratively unique identifier for an SNMP engine. (This setting is optional.) You can find the engine ID in the `/config/net-snmp/snmpd.conf` file on the BIG-IP system. Please note that this ID is identified in the file as the value of the oldEngineID token.

9. From the **Authentication Protocol** list, select the algorithm the system uses to authenticate SNMP v3 traps.

   When you set this value, you must also enter a value in the **Authentication Password** field.

10. In the **Authentication Password** field, type the password the system uses to handle an SNMP v3 trap.

    When you set this value, you must also select a value from the **Authentication Protocol** list.

    Note: *The authentication password must be at least 8 characters long.*

11. If you selected **Auth and Privacy** from the **Security Level** list, from the **Privacy Protocol** list, select the algorithm the system uses to encrypt SNMP v3 traps. When you set this value, you must also enter a value in the **Privacy Password** field.
12. If you selected **Auth and Privacy** from the **Security Level** list, in the **Privacy Password** field, type the password the system uses to handle an encrypted SNMP v3 trap. When you set this value, you must also select a value from the **Privacy Protocol** list.

    Note: *The authentication password must be at least 8 characters long.*

13. Click **Finished**.

Viewing pre-configured SNMP traps

Verify that your user account grants you access to the advanced shell.

Pre-configured traps are stored in the `/etc/alertd/alert.conf` file. View these SNMP traps to understand the data that the SNMP manager can use.

Use this command to view the SNMP traps that are pre-configured on the BIG-IP® system: `cat /etc/alertd/alert.conf`.

Creating custom SNMP traps

Verify that your user account grants you access to tmsh.

Create custom SNMP traps that alert the SNMP manager to specific SNMP events that occur on the network when the pre-configured traps do not meet all of your needs.

1. Log in to the command line.
2. Create a backup copy of the file `/config/user_alert.conf`, by typing this command: `cp /config/user_alert.conf` *`backup_file_name`*
   For example, type: `cp /config/user_alert.conf /config/user_alert.conf.backup`
3. With a text editor, open the file `/config/user_alert.conf`.
4. Add a new SNMP trap.

   The required format is:

```
alert alert_name "matched message" {
    snmptrap OID=".1.3.6.1.4.1.3375.2.4.0.XXX"
   }
```

- *alert_name* represents a descriptive name. The *alert_name* or *matched_message* value cannot match the corresponding value in any of the SNMP traps defined in the /etc/alertd/alert.conf or /config/user_alert.conf file.
- *matched_message* represents the text that matches the Syslog message that triggers the custom trap. You can specify either a portion of the Syslog message text or use a regular expression. Do not include the Syslog prefix information, such as the date stamp and process ID, in the match string.
- The *XXX* portion of the OID value represents a number that is unique to this OID. Specify any OID that meets all of these criteria:
  - Is in standard OID format and within the range .1.3.6.1.4.1.3375.2.4.0.300 through .1.3.6.1.4.1.3375.2.4.0.999.
  - Is in a numeric range that can be processed by your trap receiving tool.
  - Does not exist in the MIB file /usr/share/snmp/mibs/F5-BIGIP-COMMON-MIB.txt.
  - Is not used in another custom trap.

As an example, to create a custom SNMP trap that is triggered whenever the system logs switchboard failsafe status changes, add the following trap definition to /config/user_alert.conf.

```
alert SWITCHBOARD_FAILSAFE_STATUS "Switchboard Failsafe (.*)" {
         snmptrap OID=".1.3.6.1.4.1.3375.2.4.0.500"
    }
```

This trap definition causes the system to log the following message to the file /var/log/ltm, when switchboard failsafe is enabled: Sep 23 11:51:40 bigip1.askf5.com lacpd[27753]: 01160016:6: Switchboard Failsafe enabled.

5. Save the file.
6. Close the text editor.
7. Restart the alertd daemon by typing this command: bigstart restart alertd

   If the alertd daemon fails to start, examine the newly-added trap entry to ensure that the format is correct.

Overview: About troubleshooting SNMP traps

When the BIG-IP® alert system and the SNMP agent send traps to the SNMP manager, you can respond to the alert using the recommended actions for each SNMP trap.

AFM-related traps and recommended actions

This table provides information about the AFM™-related notifications that an SNMP manager can receive.

Trap name	Description	Recommended action
BIGIP_TMM_TMMERR_DOS_ATTACK_START (.1.3.6.1.4.1.3375.2.4.0.133)	The start of a possible DoS attack was registered.	Determine your response to this type of DoS attack, if required.

Trap name	Description	Recommended action
BIGIP_TMM_TMMERR_DOS_ATTACK_STOP (.1.3.6.1.4.1.3375.2.4.0.134)	The end of a possible DoS attack was detected.	None, informational.
BIGIP_DOSPROTECT_DOSPROTECT_AGGRREAPEROID (.1.3.6.1.4.1.3375.2.4.0.22)	The flow sweeper started or stopped.	None, informational.

ASM-related traps and recommended actions

This table provides information about the ASM™-related notifications that an SNMP manager can receive.

Trap name	Description	Recommended action
bigipAsmRequestBlocked (.1.3.6.1.4.1.3375.2.4.0.38)	The BIG-IP® system blocked an HTTP request because the request contained at least one violation to the active security policy.	Check the HTTP request to determine the cause of the violation.
bigipAsmRequestViolation (.1.3.6.1.4.1.3375.2.4.0.39)	The BIG-IP system issued an alert because an HTTP request violated the active security policy.	Check the HTTP request to determine the cause of the violation.
bigipAsmFtpRequestBlocked (.1.3.6.1.4.1.3375.2.4.0.79)	The BIG-IP system blocked an FTP request because the request contained at least one violation to the active security policy.	Check the FTP request to determine the cause of the violation.
bigipAsmFtpRequestViolation (.1.3.6.1.4.1.3375.2.4.0.80)	The BIG-IP system issued an alert because an FTP request violated the active security policy.	Check the FTP request to determine the cause of the violation.
bigipAsmSmtpRequestBlocked (.1.3.6.1.4.1.3375.2.4.0.85)	The BIG-IP system blocked an SMTP request because the request contained at least one violation to the active security policy.	Check the SMTP request to determine the cause of the violation.
bigipAsmSmtpRequestViolation (.1.3.6.1.4.1.3375.2.4.0.86)	The BIG-IP system issued an alert because an SMTP request violated the active security policy.	Check the SMTP request to determine the cause of the violation.
bigipAsmDosAttackDetected (.1.3.6.1.4.1.3375.2.4.0.91)	The BIG-IP system detected a denial-of-service (DoS) attack.	Determine the availability of the application by checking the response time of the site. Check the BIG-IP ASM logs: • Identify the source IP of the attack and observe other violations from the same source. Determine if the source IP is

Trap name	Description	Recommended action
		attacking other resources. Consider blocking the source IP in the ACL. • Identify the URL that is under attack. Consider disabling the URL, if the attack is not mitigated quickly.
bigipAsmBruteForceAttackDetected (.1.3.6.1.4.1.3375.2.4.0.92)	The BIG-IP system detected a brute force attack.	Check the BIG-IP ASM logs: • Identify the source IP of the attack and observe other violations from the same source. Determine if the source IP is attacking other resources. Consider blocking the source IP in the ACL. • Identify the user name that is under attack. Consider contacting the user and locking their account.

Application Visibility and Reporting-related traps and recommended actions

This table provides information about the Application Visibility and Reporting (AVR) notifications that an SNMP manager can receive.

Trap name	Description	Recommended action
bigipAvrAlertsMetricSnmp (.1.3.6.1.4.1.3375.2.4.0.105)	A BIG-IP system AVR SNMP metric changed.	Information only, no action required.
bigipAvrAlertsMetricSmtp (.1.3.6.1.4.1.3375.2.4.0.106)	A BIG-IP system AVR SMTP metric changed.	Information only, no action required.

Authentication-related traps and recommended actions

This table provides information about the authentication-related notifications that an SNMP manager can receive.

Trap Name	Description	Recommended Action
bigipTamdAlert (.1.3.6.1.4.1.3375.2.4.0.21)	More than 60 authentication attempts have failed within one second, for a given virtual server.	Investigate for a possible intruder.
bigipAuthFailed (.1.3.6.1.4.1.3375.2.4.0.27)	A login attempt failed.	Check the user name and password.

DoS-related traps and recommended actions

This table provides information about the denial-of-service (DoS)-related notifications that an SNMP manager can receive.

Trap name	Description	Recommended action
bigipAggrReaperStateChange (.1.3.6.1.4.1.3375.2.4.0.22)	The state of the aggressive reaper has changed, indicating that the BIG-IP® system is moving to a distress mode.	Use the default denial-of-service (DoS) settings. You can also add rate filters to survive the attack.
bigipDosAttackStart (.1.3.6.1.4.1.3375.2.4.0.133)	The BIG-IP system detected a DoS attack start.	Check the attack name in the notification to determine the kind of attack that is detected.
bigipDosAttackStop (.1.3.6.1.4.1.3375.2.4.0.134)	The BIG-IP system detected a DoS attack stop.	Information only, no action required.

General traps and recommended actions

This table provides information about the general notifications that an SNMP manager can receive.

Trap name	Description	Recommended action
bigipDiskPartitionWarn (.1.3.6.1.4.1.3375.2.4.0.25)	Free space on the disk partition is less than the specified limit. By default, the limit is 30% of total disk space.	Increase the available disk space.
bigipDiskPartitionGrowth (.1.3.6.1.4.1.3375.2.4.0.26)	The disk partition use exceeds the specified growth limit. By default, the limit is 5% of total disk space.	Increase the available disk space.
bigipUpdatePriority (.1.3.6.1.4.1.3375.2.4.0.153)	There is a high priority software update available.	Download and install the software update.
bigipUpdateServer (.1.3.6.1.4.1.3375.2.4.0.154)	Unable to connect to the F5® server running update checks.	Verify the server connection settings.
bigipUpdateError (.1.3.6.1.4.1.3375.2.4.0.155)	There was an error checking for updates.	Investigate the error.

GTM-related traps and recommended actions

This table provides information about the GTM™-related notifications that an SNMP manager can receive.

Trap name	Description	Recommended action
bigipGtmBoxAvail (.1.3.6.1.4.1.3375.2.4.0.77)	The BIG-IP® system has come UP.	Information only, no action required.
bigipGtmBoxNotAvail (.1.3.6.1.4.1.3375.2.4.0.78)	The BIG-IP system has gone DOWN.	Information only, no action required.
bigipGtmBig3dSslCertExpired (.1.3.6.1.4.1.3375.2.4.0.81)	The certificate `/config/big3d/client.crt` has expired.	Replace the certificate.

Trap name	Description	Recommended action
bigipGtmBig3dSslCertWillExpire (.1.3.6.1.4.1.3375.2.4.0.82)	The certificate `/config/big3d/client.crt` will expire soon.	Replace the certificate.
bigipGtmSslCertExpired (.1.3.6.1.4.1.3375.2.4.0.83)	The certificate `/config/gtm/server.crt` has expired.	Replace the certificate.
bigipGtmSslCertWillExpire (.1.3.6.1.4.1.3375.2.4.0.84)	The certificate `/config/gtm/server.crt` will expire soon.	Replace the certificate.
bigipGtmPoolAvail (.1.3.6.1.4.1.3375.2.4.0.40)	A global traffic management pool is available.	Information only, no action required.
bigipGtmPoolNotAvail (.1.3.6.1.4.1.3375.2.4.0.41)	A global traffic management pool is not available.	Information only, no action required.
bigipGtmPoolDisabled (.1.3.6.1.4.1.3375.2.4.0.42)	A global traffic management pool is disabled.	Check the status of the pool.
bigipGtmPoolEnabled (.1.3.6.1.4.1.3375.2.4.0.43)	A global traffic management pool is enabled.	Information only, no action required.
bigipGtmLinkAvail (.1.3.6.1.4.1.3375.2.4.0.44)	A global traffic management link is available.	Information only, no action required.
bigipGtmLinkNotAvail (.1.3.6.1.4.1.3375.2.4.0.45)	A global traffic management link is not available.	Check the status of the link, as well as the relevant detailed log message.
bigipGtmLinkDisabled (.1.3.6.1.4.1.3375.2.4.0.46)	A global traffic management link is disabled.	Check the status of the link.
bigipGtmLinkEnabled (.1.3.6.1.4.1.3375.2.4.0.47)	A global traffic management link is enabled.	Information only, no action required.
bigipGtmWideIpAvail (.1.3.6.1.4.1.3375.2.4.0.48)	A global traffic management wide IP is available.	Information only, no action required.
bigipGtmWideIpNotAvail (.1.3.6.1.4.1.3375.2.4.0.49)	A global traffic management wide IP is unavailable.	Check the status of the wide IP, as well as the relevant detailed log message.
bigipGtmWideIpDisabled (.1.3.6.1.4.1.3375.2.4.0.50)	A global traffic management wide IP is disabled.	Check the status of the wide IP.
bigipGtmWideIpEnabled (.1.3.6.1.4.1.3375.2.4.0.51)	A global traffic management wide IP is enabled.	Information only, no action required.
bigipGtmPoolMbrAvail (.1.3.6.1.4.1.3375.2.4.0.52)	A global traffic management pool member is available.	Information only, no action required.
bigipGtmPoolMbrNotAvail (.1.3.6.1.4.1.3375.2.4.0.53)	A global traffic management pool member is not available.	Check the status of the pool member, as well as the relevant detailed log message.
bigipGtmPoolMbrDisabled (.1.3.6.1.4.1.3375.2.4.0.54)	A global traffic management pool member is disabled.	Check the status of the pool member.

Trap name	Description	Recommended action
bigipGtmPoolMbrEnabled (.1.3.6.1.4.1.3375.2.4.0.55)	A global traffic management pool member is enabled.	Information only, no action required.
bigipGtmServerAvail (.1.3.6.1.4.1.3375.2.4.0.56)	A global traffic management server is available.	Information only, no action required.
bigipGtmServerNotAvail (.1.3.6.1.4.1.3375.2.4.0.57)	A global traffic management server is unavailable.	Check the status of the server, as well as the relevant detailed log message.
bigipGtmServerDisabled (.1.3.6.1.4.1.3375.2.4.0.58)	A global traffic management server is disabled.	Check the status of the server.
bigipGtmServerEnabled (.1.3.6.1.4.1.3375.2.4.0.59)	A global traffic management server is enabled.	Information only, no action required.
bigipGtmVsAvail (.1.3.6.1.4.1.3375.2.4.0.60)	A global traffic management virtual server is available.	Information only, no action required.
bigipGtmVsNotAvail (.1.3.6.1.4.1.3375.2.4.0.61)	A global traffic management virtual server is unavailable.	Check the status of the virtual server, as well as the relevant detailed log message.
bigipGtmVsDisabled (.1.3.6.1.4.1.3375.2.4.0.62)	A global traffic management virtual server is disabled.	Check the status of the virtual server.
bigipGtmVsEnabled (.1.3.6.1.4.1.3375.2.4.0.63)	A global traffic management virtual server is enabled.	Information only, no action required.
bigipGtmDcAvail (.1.3.6.1.4.1.3375.2.4.0.64)	A global traffic management data center is available.	Information only, no action required.
bigipGtmDcNotAvail (.1.3.6.1.4.1.3375.2.4.0.65)	A global traffic management data center is unavailable.	Check the status of the data center, as well as the relevant detailed log message.
bigipGtmDcDisabled (.1.3.6.1.4.1.3375.2.4.0.66)	A global traffic management data center is disabled.	Check the status of the data center.
bigipGtmDcEnabled (.1.3.6.1.4.1.3375.2.4.0.67)	A global traffic management data center is enabled.	Information only, no action required.
bigipGtmAppObjAvail (.1.3.6.1.4.1.3375.2.4.0.69)	A global traffic management application object is available.	Information only, no action required.
bigipGtmAppObjNotAvail (.1.3.6.1.4.1.3375.2.4.0.70)	A global traffic management application object is unavailable.	Check the status of the application object, as well as the relevant detailed log message.
bigipGtmAppAvail (.1.3.6.1.4.1.3375.2.4.0.71)	A global traffic management application is available.	Information only, no action required.
bigipGtmAppNotAvail (.1.3.6.1.4.1.3375.2.4.0.72)	A global traffic management application is unavailable.	Check the status of the application, as well as the relevant detailed log message.

Trap name	Description	Recommended action
bigipGtmJoinedGroup (.1.3.6.1.4.1.3375.2.4.0.73)	The BIG-IP system joined a global traffic management synchronization group.	Information only, no action required.
bigipGtmLeftGroup (.1.3.6.1.4.1.3375.2.4.0.74)	The BIG-IP system left a global traffic management synchronization group.	Information only, no action required.
bigipGtmKeyGenerationExpiration (.1.3.6.1.4.1.3375.2.4.0.95)	A generation of a DNSSEC key expired.	Information only, no action required.
bigipGtmKeyGenerationRollover (.1.3.6.1.4.1.3375.2.4.0.94)	A generation of a DNSSEC key rolled over.	Information only, no action required.
bigipGtmProberPoolDisabled (.1.3.6.1.4.1.3375.2.4.0.99)	A global traffic management prober pool is disabled.	Check the status of the prober pool.
bigipGtmProberPoolEnabled (.1.3.6.1.4.1.3375.2.4.0.100)	A global traffic management prober pool is enabled.	Information only, no action required.
bigipGtmProberPoolStatusChange (.1.3.6.1.4.1.3375.2.4.0.97)	The status of a global traffic management prober pool has changed.	Check the status of the prober pool.
bigipGtmProberPoolStatusChangeReason (.1.3.6.1.4.1.3375.2.4.0.98)	The reason the status of a global traffic management prober pool has changed.	The action required is based on the reason given.
bigipGtmProberPoolMbrDisabled (.1.3.6.1.4.1.3375.2.4.0.103)	A global traffic management prober pool member is disabled.	Check the status of the prober pool member.
bigipGtmProberPoolMbrEnabled (.1.3.6.1.4.1.3375.2.4.0.104)	A global traffic management prober pool member is enabled.	Information only, no action required.
bigipGtmProberPoolMbrStatusChange (.1.3.6.1.4.1.3375.2.4.0.101)	The status of a global traffic management prober pool member has changed.	Check the status of the prober pool member.
bigipGtmProberPoolMbrStatusChangeReason (.1.3.6.1.4.1.3375.2.4.0.102)	The reason the status of a global traffic management prober pool member has changed.	The action required is based on the reason given.

Hardware-related traps and recommended actions

This table provides information about hardware-related notifications that an SNMP manager can receive. If you receive any of these alerts, contact F5® Networks technical support.

Trap name and Associated OID	Description	Recommended action
bigipAomCpuTempTooHigh (.1.3.6.1.4.1.3375.2.4.0.93)	The AOM is reporting that the air temperature near the CPU is too high.	Check the input and output air temperatures. Run an iHealth® report and troubleshoot based on the results. If the condition persists, contact F5 Networks technical support.
bigipBladeNoPower (.1.3.6.1.4.1.3375.2.4.0.88)	A blade lost power.	Contact F5 Networks technical support.

Trap name and Associated OID	Description	Recommended action
bigipBladeTempHigh (.1.3.6.1.4.1.3375.2.4.0.87)	The temperature of a blade is too high.	This trap might be spurious. If the condition persists, contact F5 Networks technical support.
bigipBladeOffline (.1.3.6.1.4.1.3375.2.4.0.90)	A blade has failed.	Remove the blade. Contact F5 Networks technical support.
bigipChmandAlertFanTrayBad (.1.3.6.1.4.1.3375.2.4.0.121)	A fan tray in a chassis is bad or was removed.	Replace the fan tray. If the condition persists, contact F5 Networks technical support.
bigipCpuTempHigh	The CPU temperature is too high.	Check the input and output air temperatures. Run an iHealth report and troubleshoot based on the results. If the condition persists, contact F5 Networks technical support.
bigipCpuFanSpeedLow (.1.3.6.1.4.1.3375.2.4.0.5)	The CPU fan speed is too low.	Check the CPU temperature. If the CPU temperature is normal, the condition is not critical. If the condition persists, contact F5 Networks technical support.
bigipCpuFanSpeedBad (.1.3.6.1.4.1.3375.2.4.0.6)	The CPU fan is not receiving a signal.	Check the CPU temperature. If the CPU temperature is normal, the condition is not critical. If the condition persists, contact F5 Networks technical support.
bigipSystemCheckAlertFanSpeedLow (.1.3.6.1.4.1.3375.2.4.0.115)	The system fan speed is too low.	This condition is critical. Replace the fan tray. These appliances do not have fan trays: 1600, 3600, 3900, EM4000, 2000, 4000. If the condition persists, contact F5 Networks technical support.
bigipSystemCheckAlertVoltageHigh (.1.3.6.1.4.1.3375.2.4.0.114)	The system voltage is too high.	Review additional error messages in the log files. Unplug the system. Contact F5 Networks technical support. ***Note:*** *This alert does not happen for standby power.*
bigipSystemCheckAlertVoltageLow (.1.3.6.1.4.1.3375.2.4.0.123)	The system voltage is too low.	Review additional error messages in the log files. Unplug the system. Contact F5 Networks technical support. ***Note:*** *This alert does not happen for standby power.*
bigipSystemCheckAlertMilliVoltageHigh (.1.3.6.1.4.1.3375.2.4.0.124)	The system milli-voltage is too high.	Review additional error messages in the log files. Unplug the system. Contact F5 Networks technical support. ***Note:*** *This alert does not happen for standby power.*

Trap name and Associated OID	Description	Recommended action
bigipSystemCheckAlertMilliVoltageLow (.1.3.6.1.4.1.3375.2.4.0.127)	The system milli-voltage is too low.	Review additional error messages in the log files. Unplug the system. Contact F5 Networks technical support. ***Note:*** *This alert does not happen for standby power.*
bigipSystemCheckAlertTempHigh (.1.3.6.1.4.1.3375.2.4.0.113)	The system temperature is too high.	Check the system and air temperatures. If the condition persists, contact F5 Networks technical support.
bigipSystemCheckAlertCurrentHigh (.1.3.6.1.4.1.3375.2.4.0.125)	The system current is too high.	Review additional error messages in the log files. Unplug the system. Contact F5 Networks technical support. ***Note:*** *This alert does not happen for standby power.*
bigipSystemCheckAlertCurrentLow (.1.3.6.1.4.1.3375.2.4.0.128)	The system current is too low.	Review additional error messages in the log files. Unplug the system. Contact F5 Networks technical support. ***Note:*** *This alert does not happen for standby power.*
bigipSystemCheckAlertPowerHigh (.1.3.6.1.4.1.3375.2.4.0.126)	The system power is too high.	Review additional error messages in the log files. Unplug the system. Contact F5 Networks technical support. ***Note:*** *This alert does not happen for standby power.*
bigipSystemCheckAlertPowerLow (.1.3.6.1.4.1.3375.2.4.0.129)	The system power is too low.	Review additional error messages in the log files. Unplug the system. Contact F5 Networks technical support. ***Note:*** *This alert does not happen for standby power.*
bigipChassisTempHigh (.1.3.6.1.4.1.3375.2.4.0.7)	The temperature of the chassis is too high.	Contact F5 Networks technical support.
bigipChassisFanBad (.1.3.6.1.4.1.3375.2.4.0.8)	The chassis fan is not operating properly.	Replace the fan tray. If the condition persists, contact F5 Networks technical support.
bigipChassisPowerSupplyBad (.1.3.6.1.4.1.3375.2.4.0.9)	The chassis power supply is not functioning properly.	Verify that the power supply is plugged in. In the case of a dual-power-supply system, verify that both power supplies are plugged in. Contact F5 Networks technical support.
bigipLibhalBladePoweredOff (.1.3.6.1.4.1.3375.2.4.0.119)	A blade is powered off.	Contact F5 Networks technical support.

Trap name and Associated OID	Description	Recommended action
bigipLibhalSensorAlarmCritical (.1.3.6.1.4.1.3375.2.4.0.120)	The hardware sensor on a blade indicates a critical alarm.	Review any additional error messages that your receive, and troubleshoot accordingly. If the condition persists, contact F5 Networks technical support.
bigipLibhalDiskBayRemoved (.1.3.6.1.4.1.3375.2.4.0.118)	A disk sled was removed from a bay.	Information only, no action required.
bigipLibhalSsdLogicalDiskRemoved (.1.3.6.1.4.1.3375.2.4.0.117)	An SSD logical disk was removed from the BIG-IP® system.	Information only, no action required.
bigipLibhalSsdPhysicalDiskRemoved (.1.3.6.1.4.1.3375.2.4.0.116)	An SSD physical disk was removed from the BIG-IP system.	Information only, no action required.
bigipRaidDiskFailure (.1.3.6.1.4.1.3375.2.4.0.96)	An disk in a RAID disk array failed.	On `www.askf5.com`, see *SOL10856: Overview of hard drive mirroring*. If the problem persists, contact F5 Networks technical support.
bigipSsdMwiNearThreshold (.1.3.6.1.4.1.3375.2.4.0.111)	An SSD disk is reaching a known wear threshold.	Contact F5 Networks technical support.
bigipSsdMwiReachedThreshold (.1.3.6.1.4.1.3375.2.4.0.112)	An SSD disk is worn out.	If this is the first alert, the disk might continue to operate for a short time. Contact F5 Networks technical support.
bigipNetLinkDown (.1.3.6.1.4.1.3375.2.4.0.24)	An interface link is down.	This alert applies to L1 and L2, which are internal links within the device connecting the CPU and Switch subsystems. These links should never be down. If this occurs, the condition is serious. Contact F5 Networks technical support.
bigipExternalLinkChange (.1.3.6.1.4.1.3375.2.4.0.37)	The status of an external interface link has changed to either UP, DOWN, or UNPOPULATED.	This occurs when network cables are added or removed, and the network is reconfigured. Determine whether the link should be down or up, and then take the appropriate action.
bigipPsPowerOn (.1.3.6.1.4.1.3375.2.4.0.147)	The power supply for the BIG-IP system was powered on.	Information only, no action required, unless this trap is unexpected. In that case, verify that the power supply is working and that system has not rebooted.
bigipPsPowerOff (.1.3.6.1.4.1.3375.2.4.0.148)	The power supply for the BIG-IP system was powered off.	Information only, no action required, unless power off was unexpected. In that case, verify that the power supply is working and that system has not rebooted.
bigipPsAbsent (.1.3.6.1.4.1.3375.2.4.0.149)	The power supply for the BIG-IP system cannot be detected.	Information only, no action required when the BIG-IP device is operating with one power supply. For BIG-IP devices with two power supplies

Trap name and Associated OID	Description	Recommended action
		installed, verify that both power supplies are functioning correctly and evaluate symptoms.
bigipSystemShutdown (.1.3.6.1.4.1.3375.2.4.0.151)	The BIG-IP system has shut down.	Information only, no action required when the shut down was expected. Otherwise, investigate the cause of the unexpected reboot.
bigipFipsDeviceError (.1.3.6.1.4.1.3375.2.4.0.152)	The FIPS card in the BIG-IP system has encountered a problem.	Contact F5 Networks technical support.

High-availability system-related traps and recommended actions

This table provides information about the high-availability system-related notifications that an SNMP manager can receive.

Trap name	Description	Recommended action
bigipStandby (.1.3.6.1.4.1.3375.2.4.0.14)	The BIG-IP® system has switched to standby mode.	Review the log files in the `/var/log` directory and then search for core files in the `/var/core` directory. If you find a core file, or find text similar to fault at location `xxxx stack trace:`, contact F5® Networks technical support.
bigipStandByFail (.1.3.6.1.4.1.3375.2.4.0.75)	In failover condition, this standby system cannot become active.	Investigate failover condition on the standby system.
bigipActive (.1.3.6.1.4.1.3375.2.4.0.15)	The BIG-IP system has switched to active mode.	Information only, no action required.
bigipActiveActive (.1.3.6.1.4.1.3375.2.4.0.16)	The BIG-IP system is in active-active mode.	Information only, no action required.
bigipFeatureFailed (.1.3.6.1.4.1.3375.2.4.0.17)	A high-availability feature has failed.	View high-availability processes and their current status.
bigipFeatureOnline (.1.3.6.1.4.1.3375.2.4.0.18)	A high-availability feature is responding.	View high-availability processes and their current status.
bigipTrafficGroupStandby (.1.3.6.1.4.1.3375.2.4.0.141)	The status of a traffic group has changed to stand by.	Information only, no action required. To determine the reason for the failover, review the LTM® log `/var/log/ltm` and search for keywords active or standby. Additionally, you can run the `tmsh` command `tmsh show sys ha-status` to view the failover conditions.
bigipTrafficGroupActive (.1.3.6.1.4.1.3375.2.4.0.142)	The status of a traffic group has changed to active.	Information only, no action required. To determine the reason for the failover, review the LTM log `/var/log/ltm` and search for keywords active or standby. Additionally, you can run the `tmsh` command `tmsh show`

Trap name	Description	Recommended action
		`sys ha-status` to view the failover conditions.
bigipTrafficGroupOffline (.1.3.6.1.4.1.3375.2.4.0.143)	The status of a traffic group has changed to offline.	Information only, no action required.
bigipTrafficGroupForcedOffline (.1.3.6.1.4.1.3375.2.4.0.144)	The status of a traffic group has changed to forced offline.	Information only, no action required.
bigipTrafficGroupDeactivate (.1.3.6.1.4.1.3375.2.4.0.145)	A traffic group was deactivated.	Information only, no action required. To determine the reason for the deactivation, review the LTM log `/var/log/ltm` and search for the keyword deactivate.
bigipTrafficGroupActivate (.1.3.6.1.4.1.3375.2.4.0.146)	A traffic group was activated.	Information only, no action required. To determine the reason for the deactivation, review the LTM log `/var/log/ltm` and search for the keyword activate.

License-related traps and recommended actions

This table provides information about the license-related notifications that an SNMP manager can receive.

Trap name	Description	Recommended action
bigipLicenseFailed (.1.3.6.1.4.1.3375.2.4.0.19)	Validation of a BIG-IP® system license has failed, or the dossier has errors.	Occurs only when first licensing the system or adding a module key (such as HTTP compression) to an existing system. If using automatic licensing, verify connectivity to the outside world, fix the dossier if needed, and try again.
bigipLicenseExpired (.1.3.6.1.4.1.3375.2.4.0.20)	The BIG-IP license has expired.	Call F5® Networks technical support.
bigipDnsRequestRateLimiterEngaged (.1.3.6.1.4.1.3375.2.4.0.139)	The BIG-IP DNS Services license is rate-limited and the system has reached the rate limit.	Call F5 Networks technical support to upgrade your license.
bigipGtmRequestRateLimiterEngaged (.1.3.6.1.4.1.3375.2.4.0.140)	The BIG-IP GTM™ license is rate-limited and the system has reached the rate limit.	Call F5 Networks technical support to upgrade your license.
bigipCompLimitExceeded (.1.3.6.1.4.1.3375.2.4.0.35)	The compression license limit is exceeded.	Purchase additional compression licensing from F5 Networks.
bigipSslLimitExceeded (.1.3.6.1.4.1.3375.2.4.0.36)	The SSL license limit is exceeded, either for transactions per second (TPS) or for megabits per second (MPS).	Purchase additional SSL licensing from F5 Networks.

LTM-related traps and recommended actions

This table provides information about the LTM®-related notifications that an SNMP manager can receive.

Trap name	Description	Recommended action
bigipUnsolicitedRepliesExceededThreshold (.1.3.6.1.4.1.3375.2.4.0.122)	The BIG-IP® system DNS cache received unsolicited query replies exceeding the configured threshold.	Check the BIG-IP system logs to determine if the system is experiencing a distributed denial-of-service (DDoS) attack.
bigipNodeRate (.1.3.6.1.4.1.3375.2.4.0.130)	A local traffic management node has received connections exceeding the configured rate-limit.	Consider provisioning more resources on the BIG-IP system for this virtual server.
bigipNodeDown (.1.3.6.1.4.1.3375.2.4.0.12)	A BIG-IP system health monitor has marked a node as down.	Check the node and the cable connection.
bigipNodeUp (.1.3.6.1.4.1.3375.2.4.0.13)	A BIG-IP system health monitor has marked a node as up.	Information, no action required.
bigipMemberRate (.1.3.6.1.4.1.3375.2.4.0.131)	A local traffic management pool member has received connections exceeding the configured rate-limit.	Consider provisioning more resources on the BIG-IP system for this virtual server.
bigipVirtualRate (.1.3.6.1.4.1.3375.2.4.0.132)	A local traffic management virtual server has received connections exceeding the configured rate-limit.	Consider provisioning more resources on the BIG-IP system for this virtual server.
bigipLtmVsAvail (.1.3.6.1.4.1.3375.2.4.0.135)	A local traffic management virtual server is available to receive connections.	Information only, no action required.
bigipLtmVsUnavail (.1.3.6.1.4.1.3375.2.4.0.136)	A local traffic management virtual server is not available to receive connections.	Check the virtual server.
bigipLtmVsEnabled (.1.3.6.1.4.1.3375.2.4.0.137)	A local traffic management virtual server has beenwas enabled.	Information only, no action required.
bigipLtmVsDisabled (.1.3.6.1.4.1.3375.2.4.0.138)	A local traffic management virtual server has beenwas disabled.	Information only, no action required.
bigipServiceDown (.1.3.6.1.4.1.3375.2.4.0.10)	A BIG-IP system health monitor has detected a service on a node to be stopped and thus marked the node as down.	Restart the service on the node.
bigipServiceUp (.1.3.6.1.4.1.3375.2.4.0.11)	A BIG-IP system health monitor has detected a service on a node to be running and has therefore marked the node as up.	Information only, no action required.

Trap name	Description	Recommended action
bigipPacketRejected (.1.3.6.1.4.1.3375.2.4.0.34)	The BIG-IP system has rejected some packets.	Check the detailed message within this trap and act accordingly.
bigipInetPortExhaustion (.1.3.6.1.4.1.3375.2.4.0.76)	The TMM has run out of source ports and cannot open new communications channels with other machines.	Either increase the number of addresses available for SNAT automapping or SNAT pools, or lower the idle timeout value if the value is excessively high.

Logging-related traps and recommended actions

This table provides information about the logging-related notifications that an SNMP manager can receive.

Trap name	Description	Recommended action
bigipLogEmerg (.1.3.6.1.4.1.3375.2.4.0.29)	The BIG-IP® system is unusable. This notification occurs when the system logs a message with the log level LOG_EMERG.	Check the detailed message within this trap and within the `/var/log` files to determine which process has the emergency. Then act accordingly.
bigipLogAlert (.1.3.6.1.4.1.3375.2.4.0.30)	The BIG-IP system requires immediate action to function properly. This notification occurs when the system logs a message with the log level LOG_ALERT.	Check the detailed message within this trap and within the `/var/log` files to determine which process has the alert situation. Then act accordingly.
bigipLogCrit (.1.3.6.1.4.1.3375.2.4.0.31)	The BIG-IP system is in critical condition. This notification occurs when the system logs a message with the log level LOG_CRIT.	Check the detailed message within this trap and within the `/var/log` files to determine which process has the critical situation. Then act accordingly.
bigipLogErr (.1.3.6.1.4.1.3375.2.4.0.32)	The BIG-IP system has some error conditions. This notification occurs when the system logs a message with the log level LOG_ERR.	Check the detailed message within this trap and within the `/var/log` files to determine which processes have the error conditions. Then act accordingly.
bigipLogWarning (.1.3.6.1.4.1.3375.2.4.0.33)	The BIG-IP system is experiencing some warning conditions. This notification occurs when the system logs a message with the log level LOG_WARNING.	Check the detailed message within this trap and within the `/var/log` files to determine which processes have the warning conditions. Then act accordingly.

Network-related traps and recommended actions

This table provides information about the network-related notifications that an SNMP manager can receive.

Trap name	Description	Recommended action
bigipARPConflict (.1.3.6.1.4.1.3375.2.4.0.23)	The BIG-IP ®system has detected an ARP advertisement for any of its own ARP-enabled addresses. This can occur for a virtual server address or a self IP address.	Check IP addresses and routes.

vCMP-related traps and recommended actions

This table provides information about the virtual clustered multiprocessing (vCMP®)-related notifications that an SNMP manager can receive.

Trap name	Description	Recommended action
bigipVcmpAlertsVcmpPowerOn (.1.3.6.1.4.1.3375.2.4.0.107)	The BIG-IP® system powered on a vCMP guest from a suspended or powered-off state.	Information only, no action required.
bigipVcmpAlertsVcmpPowerOff (.1.3.6.1.4.1.3375.2.4.0.108)	The BIG-IP system powered off a vCMP guest.	Information only, no action required.
bigipVcmpAlertsVcmpHBLost (.1.3.6.1.4.1.3375.2.4.0.109)	The BIG-IP system cannot detect a heartbeat from a vCMP guest.	Check the guest and restart, if necessary.
bigipVcmpAlertsVcmpHBDetected (.1.3.6.1.4.1.3375.2.4.0.110)	The BIG-IP system detected a heartbeat from a new or returning vCMP guest.	Information only, no action required.

VIPRION-related traps and recommended actions

This table provides information about the VIPRION®-related notifications that an SNMP manager can receive.

Trap name	Description	Recommended action
bigipClusterdNoResponse (.1.3.6.1.4.1.3375.2.4.0.89)	The cluster daemon failed to respond for 10 seconds or more.	Start the cluster daemon.
bigipClusterPrimaryChanged (.1.3.6.1.4.1.3375.2.4.0.150)	The primary cluster has changed.	Information only, no action required.

Monitoring BIG-IP System Traffic with sFlow

Overview: Configuring network monitoring with sFlow

sFlow is an industry-standard technology for monitoring high-speed switched networks. You can configure the BIG-IP® system to poll internal data sources and send data samples to an sFlow receiver. You can then use the collected data to analyze the traffic that traverses the BIG-IP system. This analysis can help you understand traffic patterns and system usage for capacity planning and charge back, troubleshoot network and application issues, and evaluate the effectiveness of your security policies.

Task summary

Perform these tasks to configure performance monitoring of the BIG-IP® system using an sFlow device.

Adding a performance monitoring sFlow receiver
Setting global sFlow polling intervals and sampling rates for data sources
Setting the sFlow polling interval and sampling rate for a VLAN
Setting the sFlow polling interval and sampling rate for a profile
Setting the sFlow polling interval for an interface
Viewing sFlow data sources, polling intervals, and sampling rates

Adding a performance monitoring sFlow receiver

Gather the IP addresses of the sFlow receivers that you want to add to the BIG-IP® system configuration. You can use IPv4 and IPv6 addresses.

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.*

Add an sFlow receiver to the BIG-IP system when you want to use the receiver to monitor system performance.

1. On the Main tab, click **System** > **sFlow** > **Receiver List**.
   The sFlow screen opens.
2. Click **Add**.
   The New Receiver properties screen opens.
3. In the **Name** field, type a name for the sFlow receiver.
4. In the **Address** field, type the IPv4 or IPv6 address on which the sFlow receiver listens for UDP datagrams.

   Note: *The IP address of the sFlow receiver must be reachable from a self IP address on the BIG-IP system.*

   ---

5. From the **State** list, select **Enabled**.
6. Click **Finished**.

Setting global sFlow polling intervals and sampling rates for data sources

You can configure the global sFlow polling intervals and sampling rates for data sources on the BIG-IP® system, only if you are assigned either the Resource Administrator or Administrator user role.

You can configure separate sFlow global polling intervals for the system, VLANs, interfaces, and HTTP profiles, and separate sFlow global sampling rates for VLANs and HTTP profiles.

1. On the Main tab, click **System** > **sFlow** > **Global Settings**.
   The sFlow screen opens.
2. In the Name column, click a type of data source.
   The properties screen for that type of data source opens.
3. In the **Polling Interval** field, type the maximum interval in seconds between polling by the sFlow agent.
4. In the **Sampling Rate** field, type the ratio of packets observed to the number of samples you want the BIG-IP system to generate.

   For example, a sampling rate of 2000 specifies that one sample will be randomly generated for every 2000 packets observed.
5. Click **Update**.
6. Repeat this procedure to set the global polling interval and sampling rate for the other types of data sources.

Note: *You cannot configure sampling rates for the system or interface data sources.*

Setting the sFlow polling interval and sampling rate for a VLAN

You can configure the sFlow polling interval and sampling rate for a specific VLAN, only if you are assigned either the Resource Administrator or Administrator user role.

Change the sFlow settings for a specific VLAN when you want the traffic flowing through the VLAN to be sampled at a different rate than the global sFlow settings on the BIG-IP® system.

1. On the Main tab, click **Network** > **VLANs**.
   The VLAN List screen opens.
2. Click a name in the Name column.
   The New VLAN screen opens.
3. From the **Polling Interval** list, select **Specify**, and type the maximum interval in seconds between polling by the sFlow agent of this VLAN.
4. From the **Sampling Rate** list, select **Specify**, and type the ratio of packets observed at this VLAN to the samples you want the BIG-IP system to generate.

   For example, a sampling rate of 2000 specifies that 1 sample will be randomly generated for every 2000 packets observed.
5. Click **Update**.

Setting the sFlow polling interval and sampling rate for a profile

You can configure the sFlow polling interval and sampling rate for an HTTP profile, only if you are assigned either the Resource Administrator or Administrator user role.

Change the sFlow settings for a specific HTTP profile when you want the traffic flowing through the virtual server (to which the profile is assigned) to be sampled at a different rate than the global sFlow settings on the BIG-IP® system.

1. On the Main tab, click **Local Traffic** > **Profiles** > **Services** > **HTTP**.
   The HTTP profile list screen opens.
2. Click the name of a profile.
3. From the **Polling Interval** list, select **Specify**, and type the maximum interval in seconds between polling by the s Flow agent of this profile.
4. From the **Sampling Rate** list, select **Specify**, and type the ratio of packets observed at the virtual server associated with this profile to the samples you want the BIG-IP system to generate.

   For example, a sampling rate of 2000 specifies that one sample will be randomly generated for every 2000 packets observed.
5. Click **Update**.

Setting the sFlow polling interval for an interface

You can configure the sFlow polling interval for a specific interface, only if you are assigned either the Resource Administrator or Administrator user role.

Change the sFlow settings for a specific interface when you want the traffic flowing through the interface to be sampled at a different rate than the global sFlow settings on the BIG-IP® system.

1. On the Main tab, click **Network** > **Interfaces** > **Interface List**.
   The Interface List screen displays the list of interfaces on the system.
2. In the Name column, click an interface number.
   This displays the properties of the interface.
3. From the **Polling Interval** list, select **Specify**, and type the maximum interval in seconds between polling by the sFlow agent of this interface.
4. Click the **Update** button.

Viewing sFlow data sources, polling intervals, and sampling rates

You can view details about the data sources that the BIG-IP® system can poll for information to send to your sFlow receivers. For example, you can view current polling intervals and sampling rates, or determine if you want to add or remove specific data sources.

1. On the Main tab, click **System** > **sFlow** > **Data Sources**.
   The sFlow Data Sources HTTP screen opens. You can view information about the virtual server that is the data source.
2. On the menu bar, click **Data Sources**, and select **Interfaces**.
   The sFlow Data Sources HTTP screen opens. You can view information about the interface that is the sFlow data source.
3. On the menu bar, click **Data Sources**, and select **System**.
   The sFlow Data Sources HTTP screen opens. You can view information about the system that is the sFlow data source.
4. On the menu bar, click **Data Sources** and select **VLAN**.
   =The sFlow Data Sources HTTP screen opens. You can view information about the VLAN that is the sFlow data source.

sFlow receiver settings

This table names and describes the sFlow receiver settings in the Configuration utility.

Control	Default	Description
Name	no default	Specifies a name for the sFlow receiver.
Address	no default	Specifies the IP address on which the sFlow receiver listens for UDP datagrams.
Port	`6343`	Specifies the port on which the sFlow receiver listens for UDP datagrams. The default value is the standard sFlow port.
Maximum Datagram Size	`1400`	Specifies the maximum size in bytes of the UDP datagram the sFlow receiver accepts.
State	`Disabled`	Specifies whether the sFlow receiver is enabled or disabled.

sFlow global settings

This table names and describes the sFlow global settings in the Configuration utility.

Control	Default	Description
Name	Based on the resource you select.	Specifies the type of resource for which you are setting the global sFlow polling interval or sampling rate, for example, interface or vlan.
Polling Interval	`10`	Specifies the maximum interval in seconds between polling by the sFlow agent of monitored data sources on the BIG-IP system. ***Important:*** *When multiple sFlow receivers are configured on the BIG-IP® system, only the lowest, non-zero* ***Polling Interval*** *setting is used for polling for all configured sFlow receivers. Therefore, if you delete the sFlow receiver with the lowest, non-zero poll interval, the system computes a new poll interval, based on the configured sFlow receivers, and uses that polling interval for all configured sFlow receivers.*
Sampling Rate	`1024`	Specifies the ratio of packets observed to the number of samples you want the BIG-IP system to generate. For example, a sampling rate of 2000 specifies that one sample will be randomly generated for every 2000 packets observed.

sFlow counters and data

This table names and categorizes the sFlow counters and informational data that the BIG-IP® system sends to sFlow receivers. Note that the resource type corresponds to the value in the **Name** column on the sFlow global settings screen. The table also includes the source of the data and an example value.

Counter name (resource type)	Source	Example value
ifIndex (interface)	interface_stat.if_index	64 (You can map this value to an interface name by using `snmpwalk` to query `ifTable`, for example, `snmpwalk -v 2c -c public localhost ifTable`.)
ifIndex (vlan)	ifc_stats.if_index	112 (You can map this value to a VLAN name by using `snmpwalk` to query `ifTable`, for example, `snmpwalk -v 2c -c public localhost ifTable`.)
networkType (interface)	Enumeration derived from the IANAifType-MIB (http://www.iana.org/assignments/ianaiftype-mib)	6
networkType (vlan)	Enumeration derived from the IANAifType-MIB (http://www.iana.org/assignments/ianaiftype-mib)	6
ifDirection (interface)	Derived from MAU MIB (RFC 2668) 0 = unknown, 1=full-duplex, 2=half-duplex, 3 = in, 4=out	1
ifDirection (vlan)	Derived from MAU MIB (RFC 2668) 0 = unknown, 1=full-duplex, 2=half-duplex, 3 = in, 4=out	1
ifStatus (interface)	Bit field with the following bits assigned: bit 0 = ifAdminStatus (0 = down, 1 = up), bit 1 = ifOperStatus (0 = down, 1 = up)	3
ifStatus (vlan)	Bit field with the following bits assigned: bit 0 = ifAdminStatus (0 = down, 1 = up), bit 1 = ifOperStatus (0 = down, 1 = up)	3
ifInOctets (interface)	interface_stat.counters.bytes_in	9501109483
ifInOctets (vlan)	ifc_stats.hc_in_octets	107777746
ifInUcastPkts (interface)	interface_stat.counters.pkts_in - interface_stat.counters.mcast_in - interface_stat.rx_broadcast	54237438
ifInUcastPkts (vlan)	ifc_stats.hc_in_ucast_pkts	202314
ifInMulticastPkts (interface)	interface_stat.counters.mcast_in	72
ifInMulticastPkts (vlan)	ifc_stats.hc_in_multicast_pkts	343987
ifInBroadcastPkts (interface)	interface_stat.rx_broadcast	211
ifInBroadcastPkts (vlan)	ifc_stats.hc_in_broadcast_pkts	234
ifInDiscards (interface)	interface_stat.counters.drops_in	13
ifInDiscards (vlan)	ifc_stats.in_discards	13
ifInErrors (interface)	interface_stat.counters.errors_in	0

Counter name (resource type)	Source	Example value
ifInErrors (vlan)	ifc_stats.in_errors	0
ifInUnknownProtos (interface)	Unknown counter	4294967295
ifInUnknownProtos (vlan)	ifc_stats.in_unknown_protos	0
ifOutOctets (interface)	interface_stat.counters.bytes_out	9655448619
ifOutOctets (vlan)	ifc_stats.hc_out_octets	107777746
ifOutUcastPkts (interface)	interface_stat.counters.pkts_out - interface_stat.counters.mcast_out - interface_stat.tx_broadcast	10838396
ifOutUcastPkts (vlan)	ifc_stats.hc_out_ucast_pkts	202314
ifOutMulticastPkts (interface)	interface_stat.counters.mcast_out	72
ifOutMulticastPkts (vlan)	ifc_stats.hc_out_multicast_pkts	343987
ifOutBroadcastPkts (interface)	interface_stat.tx_broadcast	211
ifOutBroadcastPkts (vlan)	ifc_stats.hc_out_broadcast_pkts	234
ifOutDiscards (interface)	interface_stat.counters.drops_out	8
ifOutDiscards (vlan)	ifc_stats.out_discards	13
ifOutErrors (interface)	interface_stat.counters.errors_out	0
ifOutErrors (vlan)	ifc_stats.out_errors	0
ifPromiscuousMode (interface)	Always set to 2 (false)	2
ifPromiscuousMode (vlan)	Always set to 2 (false)	2
ifSpeed (interface)	An estimate of the current bandwidth of the interface in bits per second	1000000000
ifSpeed (vlan)	Unknown gauge	0
5s_cpu (system)	cpu_info_stat.five_sec_avg.user +cpu_info_stat.five_sec_avg.nice +cpu_info_stat.five_sec_avg.system +cpu_info_stat.five_sec_avg.iowait +cpu_info_stat.five_sec_avg.irq +cpu_info_stat.five_sec_avg.softirq +cpu_info_stat.five_sec_avg.stolen	(This value is the average system CPU usage in the last five seconds.)
1m_cpu (system)	cpu_info_stat.one_min_avg.user + cpu_info_stat.one_min_avg.nice + cpu_info_stat.one_min_avg.system + cpu_info_stat.one_min_avg.iowait + cpu_info_stat.one_min_avg.irq + cpu_info_stat.one_min_avg.softirq + cpu_info_stat.one_min_avg.stolen	(This value is the average system CPU usage in the last one minute.)

Counter name (resource type)	Source	Example value
5m_cpu (system)	cpu_info_stat.five_min_avg.user +cpu_info_stat.five_min_avg.nice +cpu_info_stat.five_min_avg.system +cpu_info_stat.five_min_avg.iowait +cpu_info_stat.five_min_avg.irq +cpu_info_stat.five_min_avg.softirq +cpu_info_stat.five_min_avg.stolen	(This value is the average system CPU usage in the last five minutes.)
total_memory_bytes (system)	tmm_stat.memory_total	5561647104 (This value is the total tmm memory in bytes.)
free_memory_bytes (system)	tmm_stat.memory_total - tmm_stat.memory_used (free tmm memory in bytes)	5363754680 (This value is the free tmm memory in bytes.)
method_option_count (http)	[profile_http_stat.options_reqs]	100
method_get_count (http)	[profile_http_stat.get_reqs]	100
method_head_count (http)	[profile_http_stat.head_reqs]	100
method_post_count (http)	[profile_http_stat.post_reqs]	100
method_put_count http)	[profile_http_stat.put_reqs]	100
method_delete_count (http)	[profile_http_stat.delete_reqs]	100
method_trace_count (http)	[profile_http_stat.trace_reqs]	100
method_connect_count (http)	[profile_http_stat.connect_reqs]	100
method_other_count (http)	[counters.number_reqs - (counters.options_reqs + counters.get_reqs + counters.head_reqs + counters.post_reqs + counters.put_reqs + counters.delete_reqs + counters.trace_reqs + counters.connect_reqs)]	20
status_1XX_count (http)	[profile_http_stat.resp_1xx.cnt]	100
status_2XX_count (http)	[profile_http_stat. resp_2xx_cnt]	80
status_3XX_count (http)	[profile_http_stat. resp_3xx_cnt]	5
status_4XX_count (http)	[profile_http_stat. resp_4xx_cnt]	1
status_5XX_count (http)	[profile_http_stat. resp_5xx_cnt]	2
status_other_count (http)	[profile_http_stat.resp_other]	100

sFlow HTTP Request sampling data types

This table names and categorizes the sFlow HTTP Request sampling data types that the BIG-IP® system sends to sFlow receivers.

Data type	Description
sampleType_tag	A numeric value that indicates the type of traffic being sampled.
sampleType	The name of the type of traffic being sampled.
sampleSequenceNo	An integer that increments with each flow sample generated per `sourceid`.
sourceId	A decimal representation in which the type of sFlow data source is indicated by one of these bytes: • 0 = ifIndex • 1 = smonVlanDataSource • 2 = entPhysicalEntry • 3 = entLogicalEntry ***Note:*** *Bytes 1-3 contain the relevant index value. On the BIG-IP system, this is the vs-index (for virtual servers) or if-index (for interfaces/vlans).*
meanSkipCount	The configured HTTP request sampling rate.
samplePool	The total number of packets that could have been sampled, that is, the number of packets skipped by the sampling process, plus the total number of samples.
dropEvents	The number of times the BIG-IP system detected that a packet marked to be sampled was dropped due to lack of resources.
inputPort	The if-index of the VLAN that the sampled packet was received on. The value of this field in combination with `outputPort` indicates the service direction.
outputPort	The if-index of the VLAN that the sampled packet was sent out on. The value of this field in combination with `inPort` indicates the service direction. ***Note:*** *1073741823 is used when the VLAN ID is unknown.*
flowBlock_tag	An sFlow standard structure ID as defined here: *http://www.slfow.org/developers/steructurs.php*. The value is in this format: Enterprise:Format, for example, 0:1.
extendedType	A string representation of the `flowBlock_tag`.
proxy_socket4_ip_protocol	The IP protocol used for communications between the BIG-IP system and the pool member that handled the traffic. The value is an integer, for example, TCP =6 and UDP =17.
proxy_socket4_local_ip	The internal IP address of the BIG-IP system.
proxy_socket4_remote_ip	The IP address of the pool member that handled the traffic.

Data type	Description
proxy_socket4_local_port	The internal port on the BIG-IP system.
proxy_socket4_remote_port	The internal port of the pool member that handled the traffic.
socket4_ip_protocol	The IP protocol used for communications between the BIG-IP system and the client represented by an integer, for example, TCP =6 and UDP=17.
socket4_local_ip	The external IP address the BIG-IP system uses to communicate with the client.
socket4_remote_ip	The IP address of the client.
socket4_local_port	The external port the BIG-IP system uses to communicate with the client.
socket4_remote_port	The port of the client.
flowSampleType	The type of traffic being sampled.
http_method	The HTTP method in the request header that was sampled.
http_protocol	The version of the HTTP protocol in the request header that was sampled.
http_uri	The URI in the request header that was sampled.
http_host	The host value in the request header that was sampled.
http_referrer	The referrer value in the request header that was sampled.
http_useragent	The User-Agent value in the request header that was sampled.
http_xff	The X-Forwarded-For value in the request header that was sampled.
http_authuser	The identity of the user in the request header as stated in *RFC 1413*.
http_mime-type	The Mime-Type of response sent to the client.
http_req_bytes	The length of the request that was sampled in bytes.
http_bytes	The length of the response that was sampled in bytes.
http_duration_uS	The duration of the communication between the BIG-IP system and the HTTP server/pool member in microseconds.
http_status	The HTTP status code in the response that was sampled.

This is an example of IPv4 HTTP Request sampling data:

```
startDatagram =================
datagramSourceIP 10.0.0.0
datagramSize 376
unixSecondsUTC 1370017719
datagramVersion 5
```

```
agentSubId 3
agent 192.27.88.20
packetSequenceNo 16
sysUpTime 1557816000
samplesInPacket 1
startSample --------------------
sampleType_tag 0:1
sampleType FLOWSAMPLE
sampleSequenceNo 1
sourceId 3:2
meanSkipCount 1
samplePool 1
dropEvents 0
inputPort 352
outputPort 1073741823
flowBlock_tag 0:2102
extendedType proxy_socket4
proxy_socket4_ip_protocol 6
proxy_socket4_local_ip 10.1.0.0
proxy_socket4_remote_ip 10.1.0.0
proxy_socket4_local_port 40451
proxy_socket4_remote_port 80
flowBlock_tag 0:2100
extendedType socket4
socket4_ip_protocol 6
socket4_local_ip 10.0.0.0
socket4_remote_ip 10.0.0.0
socket4_local_port 80
socket4_remote_port 40451
flowBlock_tag 0:2206
flowSampleType http
http_method 2
http_protocol 1001
http_uri /index.html
http_host 10.10.10.250
http_referrer http://asdfasdfasdf.asdf
http_useragent curl/7.19.7 (x86_64-redhat-linux-gnu) libcurl/7.19.7
 NSS/3.13.1.0 zlib/1.2.3 libidn/1.18 libssh2/1.2.2
http_authuser Aladdin
http_mimetype text/html; charset=UTF-8
http_request_bytes 340
http_bytes 8778
http_duration_uS 1930
http_status 200
endSample   ----------------------
endDatagram =======================
```

sFlow VLAN sampling data types

This table names and categorizes the sFlow VLAN sampling data types that the BIG-IP® system sends to sFlow receivers.

Data type	Description
sampleType_tag	A numeric value for the type of traffic being sampled.
sampleType	The name of the type of traffic being sampled.
sampleSequenceNo	An integer that increments with each flow sample generated per `sourceid`.
sourceId	A decimal value in which the type of sFlow data source is indicated by one of the bytes: • 0 = ifIndex • 1 = smonVlanDataSource

Data type	Description
	• 2 = entPhysicalEntry • 3 = entLogicalEntry ***Note:*** *Bytes 1-3 contain the relevant index value. On the BIG-IP system, this is the vs-index (for virtual servers) and the if-index (for interfaces/VLANs).*
meanSkipCount	The configured packet sampling rate.
samplePool	The total number of packets that could have been sampled, that is, the number of packets skipped by the sampling process, plus the total number of samples.
dropEvents	The number of times the BIG-IP system detected that a packet marked to be sampled was dropped due to lack of resources.
inputPort	The if-index of the VLAN that the sampled packet was received on. The value of this field in combination with `outputPort` indicates the service direction.
outputPort	The if-index of the VLAN that the sampled packet was sent out on. The value of this field in combination with `inPort` indicates the service direction. ***Note:*** *1073741823 is used when the VLAN ID is unknown.*
flowBlock_tag	An sFlow standard structure ID as defined here: *http://www.slfow.org/developers/steructurs.php*, and in this format: Enterprise:Format, for example, 0:1.
flowSampleType	The type of traffic being sampled.
headerProtocol	A numeric value for the type of header.
sampledPacketSize	The size in bytes of the packet that was sampled.
strippedBytes	The number of octets removed from the packet before extracting the header octets.
headerLen	The length of the header in bytes.
headerBytes	The exact bytes extracted from the header.
IPSize	The size of the packet that was sampled including the IP header.
ip.tot_len	The original length of the packet before sampling.
srcIP	The source IP address of the sampled packet.
dstIP	The destination IP address of the sampled packet.
IPProtocol	The protocol used to send the packet.
IPTOS	A numeric value representing the type of service.
IPTTL	The time to live of the IP address in the header of the packet that was sampled.

Data type	Description
TCPSrcPort or UDPSrcPort	The port the client uses for communication with the BIG-IP system.
TCPDstPort or UDPDstPort	The port the BIG-IP system uses for communication with the client.
TCPFlags	A decimal representation of the TCP header flags in the sampled packet. ***Note:*** *This value is sent only when the sampled traffic is TCP.*
extendedType	A string representation of the `flowBlock_tag`.
in_vlan	A numeric ID for the 8021.1Q VLAN ID of the incoming frame.
in_priority	A numeric value that represents the 802.1p priority of the incoming frame.
out_vlan	A numeric ID for the 8021.1Q VLAN ID of the outgoing frame.
out_priority	A numeric value that represents the 802.1p priority of the outgoing frame.

This is an example of IPv4 VLAN sampling data:

```
startDatagram =================================================
datagramSourceIP 10.0.0.0
datagramSize 180
unixSecondsUTC 1370016982
datagramVersion 5
agentSubId 2
agent 192.27.88.20
packetSequenceNo 1
sysUpTime 1557079000
samplesInPacket 1
startSample ----------------------------------------------------
sampleType_tag 0:1
sampleType FLOWSAMPLE
sampleSequenceNo 1
sourceId 0:352
meanSkipCount 128
samplePool 38
dropEvents 0
inputPort 352
outputPort 1073741823
flowBlock_tag 0:1
flowSampleType HEADER
headerProtocol 1
sampledPacketSize 66
strippedBytes 0
headerLen 64
headerBytes 00-01-D7-E6-8A-03-00-50-56-01-10-0E-08-00-45-00-00-
 34-D8-A4-40-00-40-06-39-10-0A-0A-0A-02-0A-0A-0A-FA-9D-77-00-50-
 33-97-00-00-EA-00-5D-80-80-10-00-FA-AF-B0-00-00-01-01-08-0A-44-
 4B-27-FA-67-51
dstMAC 0001d7e68a03
srcMAC 00505601100e
IPSize 52
ip.tot_len 52
srcIP 10.0.0.0
```

```
dstIP 10.0.0.1
IPProtocol 6
IPTOS 0
IPTTL 64
TCPSrcPort 40311
TCPDstPort 80
TCPFlags 16
flowBlock_tag 0:1001
extendedType SWITCH
in_vlan 3195
in_priority 0
out_vlan 0
out_priority 0
endSample   ----------------------------------------------------
endDatagram   ======================================================
```

Implementation result

You now have an implementation in which the BIG-IP® system periodically sends data samples to an sFlow receiver, and you can use the collected data to analyze the performance of the BIG-IP system.

Event Messages and Attack Types

Fields in ASM Violations event messages

This table lists the fields contained in event messages that might display in ASM logs. The fields are listed in the order in which they appear in a message in the log.

Field name and type	Example value	Description
unit_hostname (string)	`bigip-4.pme-ds.f5.com`	BIG-IP system FQDN
management_ip_address (IP address)	`192.168.1.246`	BIG-IP system management IP address
http_class_name (string)	`/Common/topaz4-web4`	HTTP policy name
policy_name (string)	My security policy	Name of the security policy reporting the violation
violations (string)	Attack signature detected	Violation name
support_id (non-negative integer)	18205860747014045721	Internally-generated integer to assist with client access support
request_status (string)	Blocked	Action applied to the client request
response_code (non-negative integer)	200	The HTTP response code returned by the back-end server (application). This information is only relevant for requests that are not blocked.
ip_client (IP address)	`192.168.5.10`	Client source IP address
route_domain (non-negative integer)	0 (zero)	Route domain number
method (string)	GET	HTTP method requested by client
protocol (string)	HTTP, HTTPS	Protocol name
query_string (string)	key1=val1&key2=val2	Query sent by client; query appears in the first line of the HTTP request after the path and the question mark (?)
x_forwarded_for_header_value (string)	`192.168.5.10`	Value of the XFF HTTP header
sig_ids (positive non-zero integer)	200021069	Signature ID number
sig_names (string)	Automated client access %22wget%22	Signature name
date_time (string)	2012-09-19 13:52:29	Data and time in the format: YYYY-MM-DD HH:MM:SS

Field name and type	Example value	Description
severity (string)	Error	Severity category to which the event belongs
attack_type (string)	Non-browser client	Name of identified attack
geo_location (string)	USA/NY	Country/city location information
ip_address_intelligence (string)	Botnets, Scanners	List of IP intelligence categories found for an IP address
username (string)	Admin	User name for client session
session_id (hexadeicmal number)	a9141b68ac7b4958	TCP session ID
src_port (non-negative integer)	52974	Client protocol source port
dest_port (non-negative integer)	80	Requested service listening port number
dest_ip (IP address)	`192.168.5.11`	Requested service IP address
sub_violations (string)	Bad HTTP version, Null in request	Comma-separated list of sub-violation strings
virus_name (string)	Melissa	Virus name
uri (string)	/	URI requested by client
request (string)	`GET / HTTP/1.0\r\nUser-Agent: Wget/1.12 (linux-gnu)\r\nAccept: */*\r\nHost: 10.4.1.200\r\nConnection: Keep-Alive\r\n\r\n`	Request string sent by client
headers	Host: myhost.com; Connection: close	Found in request logs
response	HTTP/1.1 200 OK Content-type: text/html Content-Length: 7 <html/>	HTTP response from server when response logging is configured
violation_details (string)	`<?xml version='1.0' encoding='UTF-8'?> <BAD_MSG><request-violations><violation> <viol_index>14</viol_index> <viol_name>VIOL_HTTP_PROTOCOL</viol_name> <http_sanity_checks_status>65536 </http_sanity_checks_status> <http_sub_violation_status>65536 </http_sub_violation_status> <http_sub_violation> SFRUUCB2ZXJzaW9uIG5vdCBmb3VuZA= =</http_sub_violation> </violation></request-violations></BAD_MSG>`	Extended information about a violation on a transaction

ASM Violations example events

This list contains examples of events you might find in ASM logs.

Examples of ASM log messages in the ArcSight CEF format

```
<134>Sep 19 13:35:00 bigip-4.pme-ds.f5.com
ASM:CEF:0|F5|ASM|11.3.0|Successful Request|Successful Request|2|
dvchost=bigip-4.pme-ds.f5.com dvc=172.16.73.34 cs1=topaz4-web4
cs1Label=policy_name cs2=/Common/topaz4-web4 cs2Label=http_class_name
deviceCustomDate1=Sep 19 2012 11:38:36
deviceCustomDate1Label=policy_apply_date
externalId=18205860747014045699 act=passed cn1=200 cn1Label=response_code
src=10.4.1.101 spt=52963 dst=10.4.1.200 dpt=80 requestMethod=GET app=HTTP
cs5=N/A cs5Label=x_forwarded_for_header_value rt=Sep 19 2012 13:35:00
deviceExternalId=0 cs4=N/A cs4Label=attack_type cs6=N/A
cs6Label=geo_location c6a1= c6a1Label=device_address c6a2=
c6a2Label=source_address c6a3= c6a3Label=destination_address c6a4=N/A
c6a4Label=ip_address_intelligence msg=N/A
suid=2e769a9e1ea8b777 suser=N/A request=/ cs3Label=full_request
cs3=GET / HTTP/1.0\r\nUser-Agent: Wget/1.12 (linux-gnu)\r\nAccept:
*/*\r\nHost: 10.4.1.200\r\nConnection: Keep-Alive\r\n\r\n
```

```
<131>Sep 19 13:53:34 bigip-4.pme-ds.f5.com
ASM:CEF:0|F5|ASM|11.3.0|200021069|Automated client access
"wget"|5|dvchost=bigip-4.pme-ds.f5.com dvc=172.16.73.34 cs1=topaz4-web4
cs1Label=policy_name cs2=/Common/topaz4-web4 cs2Label=http_class_name
deviceCustomDate1=Sep 19 2012 13:49:25
deviceCustomDate1Label=policy_apply_date externalId=18205860747014045723
act=blocked cn1=0 cn1Label=response_code src=10.4.1.101 spt=52975
dst=10.4.1.200 dpt=80 requestMethod=GET app=HTTP cs5=N/A
cs5Label=x_forwarded_for_header_value rt=Sep 19 2012 13:53:33
deviceExternalId=0 cs4=Non-browser Client cs4Label=attack_type cs6=N/A
cs6Label=geo_location c6a1= c6a1Label=device_address
c6a2= c6a2Label=source_address c6a3= c6a3Label=destination_address
c6a4=N/A c6a4Label=ip_address_intelligence msg=N/A
suid=86c4f8bf7349cac9 suser=N/A request=/ cs3Label=full_request cs3=GET /
HTTP/1.0\r\nUser-Agent: Wget/1.12 (linux-gnu)\r\nAccept: */*\r\nHost:
10.4.1.200\r\nConnection: Keep-Alive\r\n\r\n
```

Example of ASM log message in the Remote Server format

```
<134>Sep 19 13:42:41 bigip-4.pme-ds.f5.com ASM:"",
"2012-09-19 13:42:40","10.4.1.200","80","N/A","/Common/topaz4-web4"
"N/A","10.4.1.101","10.4.1.101%0","172.16.73.34","GET",
"2012-09-19 11:38:36","topaz4-web4","HTTP","",
"GET / HTTP/1.0\r\nUser-Agent: Wget/1.12(linux-gnu)\r\nAccept: */*\r\nHost:
10.4.1.200\r\nConnection: Keep-Alive\r\n\r\n","passed",
"Response logging disabled","200","0","7514e0ee8f0eb493","Informational",
"","","52965","","18205860747014045703","bigip-4.pme-ds.f5.com","/","N/A",
"<?xml version='1.0' encoding='UTF-8'?><BAD_MSG>
<request-violations><violation><viol_index>42</viol_index>
<viol_name>VIOL_ATTACK_SIGNATURE</viol_name>
<context>request</context><sig_data>
<sig_id>200021069</sig_id><blocking_mask>4</blocking_mask>
<kw_data><buffer>VXNlci1BZ2VudDogV2dldC8xLjEyIChsaW51eC1nbn
;UpDQpBY2NlcHQ6ICovKg0KSG9zdDogMTAuNC4xLjIwMA0KQ29
ubmVjdGlvbjogS2VlcC1BbGl2ZQ0KDQo=</buffer>
<offset>0</offset><length>16</length></kw_data>
</sig_data></violation></request-violations>
</BAD_MSG>","","N/A","N/A"
```

Example of ASM log message in the Remote Syslog format

```
23003140
```

Examples of ASM log messages in the Reporting Server format

```
<134>Sep 19 13:40:27 bigip-4.pme-ds.f5.com
ASM:unit_hostname="bigip-4.pme-ds.f5.com",
management_ip_address="172.16.73.34",http_class_name="/Common/topaz4-web4",
policy_name="topaz4-web4",policy_apply_date="2012-09-19 11:38:36",
violations="",support_id="18205860747014045701",request_status="passed",
response_code="200",ip_client="10.4.1.101",route_domain="0",method="GET",
protocol="HTTP",query_string="",x_forwarded_for_header_value="N/A",
sig_ids="",sig_names="",date_time="2012-09-19 13:40:26",
severity="Informational",attack_type="",geo_location="N/A",
ip_address_intelligence="N/A",username="N/A",
session_id="98630496c8413322",src_port="52964",dest_port="80",
dest_ip="10.4.1.200",sub_violations="",virus_name="N/A",uri="/",
request="GET / HTTP/1.0\r\nUser-Agent: Wget/1.12 (linux-gnu)\r\nAccept:
*/*\r\nHost: 10.4.1.200\r\nConnection: Keep-Alive\r\n\r\n"
```

```
<134>Sep 19 13:40:27 bigip-4.pme-ds.f5.com
ASM:unit_hostname="bigip-4.pme-ds.f5.com",
management_ip_address="172.16.73.34",http_class_name="/Common/topaz4-web4",
policy_name="topaz4-web4",policy_apply_date="2012-09-19 11:38:36",
violations="",support_id="18205860747014045701",request_status="passed",
response_code="200",ip_client="10.4.1.101",route_domain="0",method="GET",
protocol="HTTP",query_string="",x_forwarded_for_header_value="N/A",
sig_ids="",sig_names="",date_time="2012-09-19 13:40:26",
severity="Informational",attack_type="",geo_location="N/A",
ip_address_intelligence="N/A",username="N/A",session_id="98630496c8413322",
src_port="52964",dest_port="80",dest_ip="10.4.1.200",sub_violations="",
virus_name="N/A",uri="/",request="GET / HTTP/1.0\r\nUser-Agent: Wget/1.12
(linux-gnu)\r\nAccept: */*\r\nHost: 10.4.1.200\r\nConnection:
Keep-Alive\r\n\r\n"
```

```
<131>Sep 19 13:52:30 bigip-4.pme-ds.f5.com
ASM:unit_hostname="bigip-4.pme-ds.f5.com",
management_ip_address="172.16.73.34",http_class_name="/Common/topaz4-web4",
policy_name="topaz4-web4",policy_apply_date="2012-09-19 13:49:25",
violations="Attack signature detected",support_id="18205860747014045721",
request_status="blocked",response_code="0",ip_client="10.4.1.101",
route_domain="0",method="GET",protocol="HTTP",query_string="",
x_forwarded_for_header_value="N/A",sig_ids="200021069",
sig_names="Automated client access %22wget%22",
date_time="2012-09-19 13:52:29",severity="Error",
attack_type="Non-browser Client",geo_location="N/A",
ip_address_intelligence="N/A",username="N/A",session_id="a9141b68ac7b4958",
src_port="52974",dest_port="80",dest_ip="10.4.1.200",sub_violations="",
virus_name="N/A",uri="/",request="GET / HTTP/1.0\r\nUser-Agent: Wget/1.12
(linux-gnu)\r\nAccept: */*\r\nHost: 10.4.1.200\r\nConnection:
Keep-Alive\r\n\r\n"
```

Fields in ASM Brute Force and Web Scraping event messages

This table lists the fields contained in event messages that might display in ASM logs. The fields are listed in alphabetical order by field name.

Field name and type	Example value	Description
act (string)	Alerted or Blocked	Action taken in response to attack

Field name and type	Example value	Description
anomaly_attack_type (string)	DoS attack or Brute Force attack	Type of attack
attack_id (integer)	12345678	Unique identifier of an attack
attack_status (string)	Started, Ended, or Ongoing	Status of an attack
current_mitigation (string)	Source IP-based client-side integrity defense, URL-based client-side integrity defense, Source IP-based rate limiting, URL-based rate limiting, or Transparent	How the attack is being mitigated
date_time (string)	2012-11-07 06:53:06, or for Arcsight: Nov 07 2012 06:53:50	Current date and time in format: YYYY-MM-DD HH:MM:SS, or for ArcSight: MMM DD YYYY HH:MM:SS
detection_average (integer)	400	Historical average of TPS, latency, or failed logins
detection_mode (string)	For DoS Attacks: TPS Increased or Latency Increased; For Brute Force Attacks: Number of Failed Logins Increased	How the attack was detected
dropped_requests (integer)	10000	Number of dropped requests
dvc (IP address)	`192.168.1.246`	BIG-IP system management IP address
dvchost (string)	`bigip-4.asm-ds.f5.com`	BIG-IP system host name
geo_location (string)	USA/NY	Country/city location information
ip_list (IP addresses)	`192.168.5.10:ny, ny, usa:150`	Comma-delineated list of attacker IP addresses in the format: client_ip_addr:geo_location:drops_counter
management_ip_address (IP address)	`192.168.1.246`	BIG-IP system management IP address
operation_mode (string)	Transparent or Blocking	Current operation mode in the security policy
policy_apply_date	2012-11-07 06:53:06, or for Arcsight: Nov 07 2012 06:53:50	The date and time the policy was last applied in the format: YYYY-MM-DD HH:MM:SS, or for ArcSight: MMM DD YYYY HH:MM:SS
policy_name (string)	My policy	Name of current active policy reporting the violation
request (URL)	`www.siterequest.com`	Login URL attacked by Brute Force attack
rt (string)	Nov 07 2012 06:53:50	Current date and time in the format: MMM DD YYYY HH:MM:SS
severity (string)	Emergency	Severity category for attacks is always: Emergency
source_ip (IP address)	`192.168.4.1:ny, ny, usa:150000`	IP address from which the attack originates in the format: client_ip_addr:geo_location:drops_counter

Field name and type	Example value	Description
src (IP address)	`192.168.4.1`	IP address from which the attack originates
unit_hostname (string)	`bigip-4.asm-ds.f5.com`	BIG-IP system FQDN
uri (string)	/	Login URL that was subject to a Brute Force attack
url_list (URLs)	`192.168.50.1:sf, ca, usa:200`	Comma-delineated list of attacked URLs in the format: client_ip_addr:geo_location:drops_counter
violation_counter (integer)	100	Number of violations
web_application_name	My PTO	Name of the web application in which the violation occurred

ASM Anomaly example events

This list contains examples of events you might find in ASM logs.

Example of ASM Anomaly log messages in the ArcSight CEF format

```
CEF:0 |F5|%s|%s|%s|%s|%d| dvchost=%s dvc=%s cs1=%s cs1Label=policy_name cs2=%s
cs2Label=web_application_name deviceCustomDate1=%s
deviceCustomDate1Label=policy_apply_date act=%s cn3=%llu cn3Label=attack_id
cs4=%s cs4Label=attack_status request=%s src=%s cs6=%s cs6Label=geo_location
cs5=%s cs5Label=detection_mode rt=%s cn1=%d cn1Label=detection_average cn2=%llu
cn2Label=dropped_requests
```

```
CEF:0 |F5|%s|%s|%s|%s|%d| dvchost=%s dvc=%s cs1=%s cs1Label=policy_name cs2=%s
cs2Label=web_application_name deviceCustomDate1=%s
deviceCustomDate1Label=policy_apply_date act=%s cn3=%llu cn3Label=attack_id
cs4=%s cs4Label=attack_status src=%s cs6=%s cs6Label=geo_location cn2=%llu
cn2Label=dropped_requests rt=%s
```

```
CEF:0 |F5|%s|%s|%s|%s|%d| dvchost=%s dvc=%s cs1=%s cs1Label=policy_name cs2=%s
cs2Label=web_application_name deviceCustomDate1=%s
deviceCustomDate1Label=policy_apply_date act=%s cn3=%llu cn3Label=attack_id
cs4=%s cs4Label=attack_status src=%s cs6=%s cs6Label=geo_location rt=%s cn2=%llu
cn2Label=dropped_requests cn4=%u cn4Label=violation_counter
```

Example of ASM Anomaly log messages in the Reporting Server format

```
unit_hostname="%s",management_ip_address="%s",web_application_name="%s",
policy_name="%s",policy_apply_date="%s",anomaly_attack_type="%s",uri="%s",
attack_id="%llu",attack_status="%s",operation_mode="%s", detection_mode="%s",
detection_average="%ld",current_mitigation="%s",ip_list="%s",url_list="%s",
date_time="%s",severity="%s"
```

```
unit_hostname="%s",management_ip_address="%s",web_application_name="%s",
policy_name="%s",policy_apply_date="%s", anomaly_attack_type="%s",
attack_id="%llu",attack_status="%s",operation_mode="%s",
source_ip="%s:%s:%llu",date_time="%s",severity="%s"
```

Example of ASM Anomaly log message in the Web Scraping format
`unit_hostname="%s",management_ip_address="%s",web_application_name="%s", policy_name="%s" policy_apply_date="%s",anomaly_attack_type="%s", attack_id="%llu",attack_status="%s",operation_mode="%s", source_ip="%s:%s:%llu:%u",date_time="%s",severity="%s"`

Fields in AFM event messages

This table lists the fields that are contained in event messages that might display in AFM logs. The fields are listed in alphabetical order by field name.

Field name and type	Example value	Description
acl_rule_name (string)	Non-browser client	Name of ACL rule
action (string)	Accept, Accept decisively, Drop, Reject, Established, Closed	Action performed
hostname (string)	FQDN	BIG-IP system FQDN
bigip_mgmt_ip (IP address)	192.168.1.246	BIG-IP system management IP address
context_name (string)	`/Common/topaz3-web3`	Name of the object to which the rule applies
context_type (string)	Global, Route Domain, Virtual Server, Self IP address, or Management port	Category of the object to which the rule applies
date_time (string)	01 11 2012 13:11:10	Date and time the event occurred in this format: MMM DD YYYY HH:MM:SS
dest_ip (IP address)	`192.168.3.1`	Destination IP address
dest_port (integer)	80	Protocol port number
device_product (string)	Advanced Firewall Module	Name of BIG-IP system generating the event message
device_vendor (string)	F5	F5 static keyword
device_version (string)	11.3.0.2012.0	BIG-IP system software version in the format version.point_release.0.yyyy.0
drop_reason (string)	(empty), <name of error>, Policy	Reason action performed.
errdefs_msgno (integer)	23003137	Event number
errdefs_msg_name (string)	Network event	Event name
ip_protocol (string)	TCP, UDP, ICMP	Name of protocol
severity (integer)	8	Level of the event by number
partition_name (string)	Common	Name of the partition or folder in which the object resides
route_domain (integer)	1	Route domain number (non-negative)

Field name and type	Example value	Description
src_ip (IP address)	192.168.3.1	Source IP address
src_port (integer)	80	Protocol port number (non-negative)
vlan (string)	External	VLAN interface name

AFM example events

This list contains examples of events you might find in AFM logs.

Examples of AFM log messages in the ArcSight CEF format

```
CEF:0|F5|Advanced Firewall Module|11.3.0.2095.0|23003137|Network Event|8|rt=Oct
04 2012 13:15:29 dvchost=bigip-3.pme-ds.f5.com dvc=192.168.73.33 src=10.3.1.101
spt=39321 dst=10.3.1.200 dpt=443 proto=TCP cs1=/Common/topaz3-all3
cs1Label=virtual_name cs2=/Common/external cs2Label=vlan act=Accept c6a2=
c6a2Label=source_address c6a3= c6a3Label=destination_address cs3=
cs3Label=drop_reason cn4=0 cn4Label=route_domain cs5=allow_https
cs5Label=acl_rule_name

CEF:0|F5|Advanced Firewall Module|11.3.0.2095.0|23003137|Network Event|8|rt=Oct
04 2012 13:15:29 dvchost=bigip-3.pme-ds.f5.com dvc=192.168.73.33 src=10.3.1.101
spt=52799 dst=10.3.1.200 dpt=80 proto=TCP cs1=/Common/topaz3-web3
cs1Label=virtual_name cs2=/Common/external cs2Label=vlan act=Open c6a2=
c6a2Label=source_address c6a3= c6a3Label=destination_address cs3=
cs3Label=drop_reason cn4=0 cn4Label=route_domain cs5= cs5Label=acl_rule_name

CEF:0|F5|Advanced Firewall Module|11.3.0.2095.0|23003137|Network Event|8|rt=Oct
04 2012 13:15:29 dvchost=bigip-3.pme-ds.f5.com dvc=192.168.73.33 src=10.3.1.101
spt=52799 dst=10.3.1.200 dpt=80 proto=TCP cs1=/Common/topaz3-web3
cs1Label=virtual_name cs2=/Common/external cs2Label=vlan act=Closed c6a2=
c6a2Label=source_address c6a3= c6a3Label=destination_address cs3=
cs3Label=drop_reason cn4=0 cn4Label=route_domain cs5= cs5Label=acl_rule_name

CEF:0|F5|Advanced Firewall Module|11.3.0.2790.300|23003137|Network Event|8|rt=Nov
08 2012 18:35:15 dvchost=asm176.labt.ts.example.com dvc=192.168.69.176 src=
spt=20 dst= dpt=80 proto=TCP cs1= cs1Label=Global cs2=/Common/VLAN10
cs2Label=vlan act=Accept c6a2=fc55::99 c6a2Label=source_address c6a3=fc55::3
c6a3Label=destination_address cs3= cs3Label=drop_reason cn4=0
cn4Label=route_domain cs5=TCP cs5Label=acl_rule_name
```

Examples of AFM log messages in the Reporting Server format

```
acl_rule_name="allow_http",action="Accept",hostname="bigip-3.pme-ds.f5.com",bigip_mgmt_ip="192.168.73.33",context_name="/Common/topaz3-web3",context_type="Virtual
Server",date_time="Oct 04 2012
13:18:04",dest_ip="10.3.1.200",dest_port="80",device_product="Advanced Firewall
Module",device_vendor="F5",device_version="11.3.0.2095.0",drop_reason="",errdefs_msgno="23003137",errdefs_msg_name="Network
Event",ip_protocol="TCP",severity="8",partition_name="Common",route_domain="0",source_ip="10.3.1.101",source_port="52807",vlan="/Common/external"

acl_rule_name="",action="Open",hostname="bigip-3.pme-ds.f5.com",bigip_mgmt_ip="192.168.73.33",context_name="/Common/topaz3-all3",context_type="Virtual
Server",date_time="Oct 04 2012
13:18:04",dest_ip="10.3.1.200",dest_port="443",device_product="Advanced Firewall
Module",device_vendor="F5",device_version="11.3.0.2095.0",drop_reason="",errdefs_msgno="23003137",errdefs_msg_name="Network
Event",ip_protocol="TCP",severity="8",partition_name="Common",route_domain="0",source_ip="10.3.1.101",source_port="39329",vlan="/Common/external"

acl_rule_name="",action="Closed",hostname="bigip-3.pme-ds.f5.com",bigip_mgmt_ip="192.168.73.33",context_name="/Common/topaz3-all3",context_type="Virtual
Server",date_time="Oct 04 2012
```

Examples of AFM log messages in the Reporting Server format

```
13:18:04",dest_ip="10.3.1.200",dest_port="443",device_product="Advanced Firewall
Module",device_vendor="F5",device_version="11.3.0.2095.0",drop_reason="",errdefs_msgno="23003137",errdefs_msg_name="Network
Event",ip_protocol="TCP",severity="8",partition_name="Common",route_domain="0",source_ip="10.3.1.101",source_port="39829",vlan="/Common/external"
```

Examples of AFM log messages in the Splunk format

```
acl_rule_name="TCP",action="Accept",hostname="asm176.labt.ts.example.com",bigip_mgmt_ip="192.168.69.176",context_name="",context_type="Global",date_time="Nov
08 2012 18:38:18",dest_ip="fc55::3",dest_port="80",device_product="Advanced
Firewall
Module",device_vendor="F5",device_version="11.3.0.2790.300",drop_reason="",errdefs_msgno="23003137",errdefs_msg_name="Network
Event",ip_protocol="TCP",severity="8",partition_name="Common",route_domain="0",source_ip="fc55::99",source_port="20",vlan="/Common/VLAN10"

acl_rule_name="",action="Drop",hostname="asm176.labt.ts.example.com",bigip_mgmt_ip="192.168.69.176",context_name="/Common/vs10_TCP_IPv6",context_type="Virtual
Server",date_time="Nov 08 2012
18:38:18",dest_ip="fc55::3",dest_port="80",device_product="Advanced Firewall
Module",device_vendor="F5",device_version="11.3.0.2790.300",drop_reason="Bad
TCP checksum",errdefs_msgno="23003137",errdefs_msg_name="Network
Event",ip_protocol="TCP",severity="8",partition_name="Common",route_domain="0",source_ip="fc55::99",source_port="20",vlan="/Common/VLAN10"
```

Example of AFM log message in the Syslog format

```
23003137 [F5@12276 acl_rule_name="TCP" action="Accept"
hostname="asm176.labt.ts.example.com" bigip_mgmt_ip="192.168.69.176"
context_name="" context_type="Global" date_time="Nov 08 2012 18:42:49"
dest_ip="fc55::3" dest_port="80" device_product="Advanced Firewall Module"
device_vendor="F5" device_version="11.3.0.2790.300" drop_reason=""
errdefs_msgno="23003137" errdefs_msg_name="Network Event" ip_protocol="TCP"
severity="8" partition_name="Common" route_domain="0" source_ip="fc55::99"
source_port="20" vlan="/Common/VLAN10"]
"192.168.69.176","asm176.labt.ts.example.com","Global","","fc55::99","fc55::3","20","80","/Common/VLAN10","TCP","0","TCP","Accept",""

23003137 [F5@12276 acl_rule_name="" action="Drop"
hostname="asm176.labt.ts.example.com" bigip_mgmt_ip="192.168.69.176"
context_name="/Common/vs10_TCP_IPv6" context_type="Virtual Server" date_time="Nov
08 2012 18:42:49" dest_ip="fc55::3" dest_port="80" device_product="Advanced
Firewall Module" device_vendor="F5" device_version="11.3.0.2790.300"
drop_reason="Bad TCP checksum" errdefs_msgno="23003137" errdefs_msg_name="Network
Event" ip_protocol="TCP" severity="8" partition_name="Common" route_domain="0"
source_ip="fc55::99" source_port="20" vlan="/Common/VLAN10"]
"192.168.69.176","asm176.labt.ts.example.com","Virtual
Server","/Common/vs10_TCP_IPv6","fc55::99","fc55::3","20","80","/Common/VLAN10","TCP","0","","Drop","Bad
TCP checksum"
```

Example of AFM log message in the Syslog BSD format

```
23003137
"192.168.69.176","asm176.labt.ts.example.com","Global","","fc55::99","fc55::3","20","80","/Common/VLAN10","TCP","0","TCP","Accept",""

23003137 "192.168.69.176","asm176.labt.ts.example.com","Virtual
Server","/Common/vs10_TCP_IPv6","fc55::99","fc55::3","20","80","/Common/VLAN10","TCP","0","","Drop","Bad
TCP checksum"
```

Example of AFM log message in the Syslog Legacy F5 format

```
Oct 04 11:20:15 bigip-3.pme-ds.f5.com tmm[18691]: 23003137
allow_dns-tcp,Accept,bigip-3.pme-ds.f5.com,/Common/topaz3-all3,Virtual Server,Oct
```

Example of AFM log message in the Syslog Legacy F5 format

```
04 2012
11:20:15,10.3.1.200,2607,,192.168.73.33,TCP,0,10.3.1.101,47910,/Common/external

Oct 04 11:20:15 bigip-3.pme-ds.f5.com tmm[18691]: 23003137
,Open,bigip-3.pme-ds.f5.com,/Common/topaz3-all3,Virtual Server,Oct 04 2012
11:20:15,10.3.1.200,1666,,192.168.73.33,TCP,0,10.3.1.101,36388,/Common/external

Oct 04 11:20:15 bigip-3.pme-ds.f5.com tmm[18691]: 23003137
,Closed,bigip-3.pme-ds.f5.com,/Common/topaz3-all3,Virtual Server,Oct 04 2012
11:20:15,10.3.1.200,1666,,192.168.73.33,TCP,0,10.3.1.101,36388,/Common/external
```

Fields in Network DoS Protection event messages

This table lists the fields that are contained in event messages that might display in the DoS Protection logs. The fields are listed in alphabetical order by field name.

Field name and type	Example value	Description
action (string)	Allow, Drop, None	Action performed or reported
hostname (string)	FQDN	BIG-IP system FQDN
bigip_mgmt_ip (IP address)	192.168.1.246	BIG-IP system management IP address
date_time (string)	01 11 2012 13:11:10	Date and time the event occurred in this format: MMM DD YYYY HH:MM:SS
dest_ip (IP address)	192.168.3.1	Destination IP address
dest_port (integer)	80	Protocol port number (non-negative)
device_product (string)	Advanced Firewall Module	Name of BIG-IP system generating the event message
device_vendor (string)	F5	F5 static keyword
device_version (string)	11.3.0.2012.0	BIG-IP system software version in the format mm.dd.0.yyyy.0
dos_attack_event (string)	Attack started, Attack Sampled, Attack Stopped	Attack instances start and stop events
dos_attack_id (string)	2760296639	Unique, non-negative, attack ID
dos_attack_name (string)	ICMP Flood, Bad TCP checksum	Network DoS event
errdefs_msgno (integer)	23003138	Static number
errdefs_msg_name (string)	Network DoS event	Static keyword
severity (integer)	8	Event severity value (non-negative integer)
partition_name (string)	Common	Name of the partition in which the virtual server resides
route_domain (integer)	1	Route domain number (non-negative)
src_ip (IP address)	192.168.3.1	Source IP address
src_port (integer)	80	Protocol port number (non-negative)

Field name and type	Example value	Description
vlan (string)	External	Name of the VLAN interface

Device DoS attack types

This table lists device DoS attacks, and provides a short description and relevant information. The attack types are listed in alphabetical order by attack name.

DoS Category	Attack Name	Dos Vector Name	Information
Bad Header - DNS	DNS Oversize	dns-oversize	Detects oversized DNS headers. To tune this value, in tmsh: `modify sys db dos.maxdnssize value`, where `value` is `256-8192`.
Bad Header - ICMP	Bad ICMP Checksum	bad-icmp-chksum	An ICMP frame checksum is bad. Reuse the TCP or UDP checksum bits in the packet
	Bad ICMP Frame	bad-icmp-frame	The ICMP frame is either the wrong size, or not of one of the valid IPv4 or IPv6 types. Valid IPv4 types: • 0 Echo Reply • 3 Destination Unreachable • 4 Source Quench • 5 Redirect • 8 Echo • 11 Time Exceeded • 12 Parameter Problem • 13 Timestamp • 14 Timestamp Reply • 15 Information Request • 16 Information Reply • 17 Address Mask Request • 18 Address Mask Reply Valid IPv6 types: • 1 Destination Unreachable • 2 Packet Too Big • 3 Time Exceeded • 4 Parameter Problem • 128 Echo Request • 129 Echo Reply • 130 Membership Query • 131 Membership Report • 132 Membership Reduction
	ICMP Frame Too Large	icmp-frame-too-large	The ICMP frame exceeds the declared IP data length or the maximum datagram length. To tune this value, in tmsh: `modify sys db dos.maxicmpframesize value`, where `value` is `<=65515`.

DoS Category	Attack Name	Dos Vector Name	Information
Bad Header - IGMP	Bad IGMP Frame	bad-igmp-frame	IPv4 IGMP packets should have a header >= 8 bytes. Bits 7:0 should be either 0x11, 0x12, 0x16, 0x22 or 0x17, or else the header is bad. Bits 15:8 should be non-zero only if bits 7:0 are 0x11, or else the header is bad.
Bad Header - IPv4	Bad IP TTL Value	bad-ttl-val	Time-to-live equals zero for an IPv4 address.
	Bad IP Version	bad-ver	The IPv4 address version in the IP header is not 4.
	Header Length > L2 Length	hdr-len-gt-l2-len	No room in layer 2 packet for IP header (including options) for IPv4 address
	Header Length Too Short	hdr-len-too-short	IPv4 header length is less than 20 bytes
	Bad Source	ip-bad-src	The IPv4 source IP = `255.255.255.255` or `0xe0000000U`
	IP Error Checksum	ip-err-chksum	The header checksum is not correct
	IP Length > L2 Length	ip-len-gt-l2-len	Total length in IPv4 address header or payload length in IPv6 address header is greater than the layer 3 length in a layer 2 packet
	TTL <= <tunable>	ttl-leq-one	An IP packet with a destination that is not multicast and that has a TTL greater than 0 and less than or equal to a tunable value, which is 1 by default. To tune this value, in tmsh: `modify sys db dos.iplowttl value`, where `value` is `1-4`.
	IP Option Frames	ip-opt-frames	IPv4 address packet with `option.db variable tm.acceptipsourceroute` must be enabled to receive IP options
	IP Option Illegal Length		Option present with illegal length
	L2 Length >> IP Length	l2-len-ggt-ip-len	Layer 2 packet length is much greater than the payload length in an IPv4 address header and the layer 2 length is greater than the minimum packet size
	No L4	no-l4	No layer 4 payload for IPv4 address
	Unknown Option Type	unk-ipopt-type	Unknown IP option type
Bad Header - IPv6	IPv6 extended headers wrong order	bad-ext-hdr-order	Extension headers in the IPv6 header are in the wrong order
	Bad IPV6 Hop Count	bad-ipv6-hop-cnt	Both the terminated (cnt=0) and forwarding packet (cnt=1) counts are bad.
	Bad IPV6 Version	bad-ipv6-ver	The IPv6 address version in the IP header is not 6
	IPv6 duplicate extension headers	dup-ext-hdr	An extension header should occur only once in an IPv6 packet, except for the Destination Options extension header.

DoS Category	Attack Name	Dos Vector Name	Information
	IPv6 extension header too large	ext-hdr-too-large	An extension header is too large. To tune this value, in tmsh: `modify sys db dos.maxipv6extsize value`, where `value` is `0-1024`.
	IPv6 hop count <= <tunable>	hop-cnt-leq-one	The IPv6 extended header hop count is less than or equal to <tunable>. To tune this value, in tmsh: `modify sys db dos.ipv6lowhopcnt value`, where `value` is `1-4`.
	Bad IPv6 source	ipv6-bad-src	IPv6 source IP = `0xff00::`
	IPV6 Extended Header Frames	ipv6-ext-hdr-frames	IPv6 address contains extended header frames
	IPV6 Length > L2 Length	ipv6-len-gt-l2-len	IPv6 address length is greater than the layer 2 length
	IPV6 Source Address == Destination Address		IPv6 packet source address is the same as the destination address
	No L4 (Extended Headers Go To Or Past End of Frame)	l4-ext-hdrs-go-end	Extended headers go to the end or past the end of the L4 frame
	Payload Length < L2 Length	payload-len-ls-l2-len	Specified IPv6 payload length is less than the L2 packet length
	Too Many Extended Headers	too-many-ext-hdrs	For an IPv6 address, there are more than <tunable> extended headers (the default is `4`). To tune this value, in tmsh: `modify sys db dos.maxipv6exthdrs value`, where `value` is `0-15`.
Bad Header - L2	Ethernet MAC Source Address == Destination Address	ether-mac-sa-eq-da	Ethernet MAC source address equals the destination address.
Bad Header - TCP	Bad TCP Checksum	bad-tcp-chksum	The TCP checksum does not match
	Bad TCP Flags (All Cleared)	bad-tcp-flags-all-clr	Bad TCP flags (all cleared and SEQ#=0)
	Bad TCP Flags (All Flags Set)	bad-tcp-flags-all-set	Bad TCP flags (all flags set)
	FIN Only Set	fin-only-set	Bad TCP flags (only FIN is set)
	Option Present With Illegal Length	opt-present-with-illegal-len	Option present with illegal length
	SYN && FIN Set	syn-and-fin-set	Bad TCP flags (SYN and FIN set)
	TCP Flags - Bad URG	tcp-bad-urg	Packet contains a bad URG flag, this is likely malicious
	TCP Header Length > L2 Length	tcp-hdr-len-gt-l2-len	

DoS Category	Attack Name	Dos Vector Name	Information
	TCP Header Length Too Short (Length < 5)	tcp-hdr-len-too-short	The Data Offset value in the TCP header is less than five 32-bit words
	TCP Option Overruns TCP Header	tcp-opt-overruns-tcp-hdr	The TCP option bits overrun the TCP header.
	Unknown TCP Option Type	unk-tcp-opt-type	Unknown TCP option type
Bad Header - UDP	Bad UDP Checksum	bad-udp-chksum	The UDP checksum is not correct
	Bad UDP Header (UDP Length > IP Length or L2 Length)	bad-udp-hdr	UDP length is greater than IP length or layer 2 length
DNS	DNS AAAA Query	dns-aaaa-query	UDP packet, DNS Qtype is AAAA, VLAN is <tunable>. To tune this value, in tmsh: `modify sys db dos.dnsvlan value`, where `value` is `0-4094`.. To tune this value, in tmsh: `modify sys db dos.dnsvlan value`, where `value` is `0-4094`.
	DNS Any Query	dns-any-query	UDP packet, DNS Qtype is ANY_QRY, VLAN is <tunable>. To tune this value, in tmsh: `modify sys db dos.dnsvlan value`, where `value` is `0-4094`.
	DNS AXFR Query	dns-axfr-query	UDP packet, DNS Qtype is AXFR, VLAN is <tunable>. To tune this value, in tmsh: `modify sys db dos.dnsvlan value`, where `value` is `0-4094`.
	DNS A Query	dns-a-query	UDP packet, DNS Qtype is A_QRY, VLAN is <tunable>. To tune this value, in tmsh: `modify sys db dos.dnsvlan value`, where `value` is `0-4094`.
	DNS CNAME Query	dns-cname-query	UDP DNS query, DNS Qtype is CNAME, VLAN is <tunable>. To tune this value, in tmsh: `modify sys db dos.dnsvlan value`, where `value` is `0-4094`.
	DNS IXFR Query	dns-ixfr-query	UDP DNS query, DNS Qtype is IXFR, VLAN is <tunable>. To tune this value, in tmsh: `modify sys db dos.dnsvlan value`, where `value` is `0-4094`.
	DNS Malformed	dns-malformed	Malformed DNS packet
	DNS MX Query	dns-mx-query	UDP DNS query, DNS Qtype is MX, VLAN is <tunable>. To tune this value, in tmsh: `modify sys db dos.dnsvlan value`, where `value` is `0-4094`.
	DNS NS Query	dns-ns-query	UDP DNS query, DNS Qtype is NS, VLAN is <tunable>. To tune this value, in tmsh: `modify`

DoS Category	Attack Name	Dos Vector Name	Information
			`sys db dos.dnsvlan value`, where `value` is `0-4094`.
	DNS OTHER Query	dns-other-query	UDP DNS query, DNS Qtype is OTHER, VLAN is <tunable>. To tune this value, in tmsh: `modify sys db dos.dnsvlan value`, where `value` is `0-4094`.
	DNS PTR Query	dns-ptr-query	UDP DNS query, DNS Qtype is PTR, VLAN is <tunable>. To tune this value, in tmsh: `modify sys db dos.dnsvlan value`, where `value` is `0-4094`.
	DNS QDCount Limit	dns-qdcount-limit	UDP packet, DNS qdcount neq 1, VLAN is <tunable>. To tune this value, in tmsh: `modify sys db dos.dnsvlan value`, where `value` is `0-4094`.
	DNS Response Flood	dns-response-flood	UDP DNS Port=53, packet and DNS header flags bit 15 is 1 (response), VLAN is <tunable>. To tune this value, in tmsh: `modify sys db dos.dnsvlan value`, where `value` is `0-4094`.;
	DNS SOA Query	dns-soa-query	UDP packet, DNS Qtype is SOA_QRY, VLAN is <tunable>. To tune this value, in tmsh: `modify sys db dos.dnsvlan value`, where `value` is `0-4094`.
	DNS SRV Query	dns-srv-query	UDP packet, DNS Qtype is SRV, VLAN is <tunable>. To tune this value, in tmsh: `modify sys db dos.dnsvlan value`, where `value` is `0-4094`.
	DNS TXT Query	dns-txt-query	UDP packet, DNS Qtype is TXT, VLAN is <tunable>. To tune this value, in tmsh: `modify sys db dos.dnsvlan value`, where `value` is `0-4094`.
Flood	ARP Flood	arp-flood	ARP packet flood
	Ethernet Broadcast Packet	ether-brdcst-pkt	Ethernet broadcast packet flood
	Ethernet Multicast Packet	ether-multicst-pkt	Ethernet destination is not broadcast, but is multicast
	ICMPv4 Flood	icmpv4-flood	Flood with ICMP v4 packets
	ICMPv6 Flood	icmpv6-flood	Flood with ICMP v6 packets
	IGMP Flood	igmp-flood	Flood with IGMP packets (IPv4 packets with IP protocol number 2)
	IGMP Fragment Flood	igmp-frag-flood	Fragmented packet flood with IGMP protocol
	IPv4 Fragment Flood	ip-frag-flood	Fragmented packet flood with IPv4
	IPv6 Fragment Flood	ipv6-frag-flood	Fragmented packet flood with IPv6

DoS Category	Attack Name	Dos Vector Name	Information
	Routing Header Type 0	routing-header-type-0	Routing header type zero is present in flood packets
	TCP BADACK Flood	tcp-ack-flood	TCP ACK packet flood
	TCP RST Flood	tcp-rst-flood	TCP RST flood
	TCP SYN ACK Flood	tcp-synack-flood	TCP SYN/ACK flood
	TCP SYN Flood	tcp-syn-flood	TCP SYN flood
	TCP Window Size	tcp-window-size	The TCP window size in packets is above the maximum. To tune this value, in tmsh: `modify sys db dos.tcplowwindowsize value`, where `value` is <=128.
	UDP Flood	udp-flood	UDP flood attack
Fragmentation	ICMP Fragment	icmp-frag	ICMP fragment flood
	IPV6 Atomic Fragment	ipv6-atomic-frag	IPv6 Frag header present with M=0 and FragOffset =0
	IPV6 Fragment Error	ipv6-other-frag	Other IPv6 fragment error
	IPv6 Fragment Overlap	ipv6-overlap-frag	IPv6 overlapping fragment error
	IPv6 Fragmentat Too Small	ipv6-short-frag	IPv6 short fragment error
	IP Fragment Error	ip-other-frag	Other IPv4 fragment error
	IP Fragment Overlap	ip-overlap-frag	IPv4 overlapping fragment error
	IP Fragment Too Small	ip-short-frag	IPv4 short fragment error
Single Endpoint	Single Endpoint Flood	flood	Flood to a single endpoint. You can configure packet types to check for, and packets per second for both detection and rate limiting
	Single Endpoint Sweep	sweep	Sweep on a single endpoint. You can configure packet types to check for, and packets per second for both detection and rate limiting
SIP	SIP ACK Method	sip-ack-method	SIP ACK packets
	SIP BYE Method	sip-bye-method	SIP BYE packets
	SIP CANCEL Method	sip-cancel-method	SIP CANCEL packets
	SIP INVITE Method	sip-invite-method	SIP INVITE packets
	SIP Malformed	sip-malformed	Malformed SIP packets
	SIP MESSAGE Method	sip-message-method	SIP MESSAGE packets

DoS Category	Attack Name	Dos Vector Name	Information
	SIP NOTIFY Method	sip-notify-method	SIP NOTIFY packets
	SIP OPTIONS Method	sip-options-method	SIP OPTIONS packets
	SIP OTHER Method	sip-other-method	SIP OTHER packets
	SIP PRACK Method	sip-prack-method	SIP PRACK packets
	SIP PUBLISH Method	sip-publish-method	SIP PUBLISH packets
	SIP REGISTER Method	sip-register-method	SIP REGISTER packets
	SIP SUBSCRIBE Method	sip-subscribe-method	SIP SUBSCRIBE packets
Other	Host Unreachable	host-unreachable	Host unreachable error
	LAND Attack	land-attack	Spoofed TCP SYN packet attack
	TIDCMP	tidcmp	ICMP source quench attack

Network DoS Protection example events

This list contains examples of events you might find in Network (layer 2 - 4) DoS Protection logs.

Example of Network DOS Protection log message in the ArcSight format

```
CEF:0|F5|Advanced Firewall Module|11.3.0.2790.300|Bad TCP
checksum|Drop|8|dvchost=asm176.labt.ts.example.com dvc=192.168.69.176 rt=Nov
08 2012 17:58:02 act=Drop cn1=3083822789 cn1Label=attack_id cs1=Attack Sampled
cs1Label=attack_status src= spt=20 dst= dpt=80 cs2=/Common/VLAN10 cs2Label=vlan
cs3= cs3Label=virtual_name cn4=0 cn4Label=route_domain c6a2=fc55::99
c6a2Label=source_address c6a3=fc55::3 c6a3Label=destination_address
```

Example of Network DoS Protection log message in the Remote Syslog format

```
"Nov 06 2012
02:17:27","192.168.69.245","asm245.labt.ts.example.com","","10.10.10.2","10.10.10.200","20","80","0","/Common/vlan1","Bad
TCP checksum","3044184075","Attack Sampled","Drop"
```

Examples of Network DoS Protection log messages in Reporting Server format

```
Oct 30 13:59:38 192.168.57.163
action="None",hostname="bigip-7.pme-ds.f5.com",bigip_mgmt_ip="192.168.73.18",date_time="Sep
20 2012 15:30:43",dest_ip="",dest_port="",device_product="Advanced Firewall
Module",device_vendor="F5",device_version="11.3.0.1910.0",dos_attack_event="Attack
Started",dos_attack_id="2760296639",dos_attack_name="Ethernet broadcast
packet",errdefs_msgno="23003138",errdefs_msg_name="Network DoS
Event",severity="8",partition_name="Common",route_domain="",source_ip="",source_port="",vlan=""
```

Examples of Network DoS Protection log messages in Reporting Server format

```
Oct 30 13:59:38 192.168.57.163
action="Drop",hostname="bigip-7.pme-ds.f5.com",bigip_mgmt_ip="192.168.73.18",date_time="Sep
20 2012 15:30:44",dest_ip="",dest_port="",device_product="Advanced Firewall
Module",device_vendor="F5",device_version="11.3.0.1910.0",dos_attack_event="Attack
Sampled",dos_attack_id="2760296639",dos_attack_name="Ethernet broadcast
packet",errdefs_msgno="23003138",errdefs_msg_name="Network DoS
Event",severity="8",partition_name="Common",route_domain="",source_ip="",source_port="",vlan="/Common/external"
```

Example of Network DoS Protection log message in the Splunk format

```
action="Blocking",hostname="bigip1",bigip_mgmt_ip="192.168.36.157",client_ip_geo_location="N/A",client_request_uri="",configuration_date_time="Nov
01 2012 04:39:57",context_name="/Common/vs_159",context_type="Virtual
Server",date_time="Nov 01 2012
05:01:40",device_product="ASM",device_vendor="F5",device_version="11.3.0",dos_attack_detection_mode="TPS
Increased",dos_attack_event="Attack
ongoing",dos_attack_id="3131200721",dos_attack_name="DOS L7
attack",dos_attack_tps="0
tps",dos_dropped_requests_count="487",dos_mitigation_action="Source IP-Based
Rate Limiting",errdefs_msgno="23003140",errdefs_msg_name="Application DoS
Event",severity="7",partition_name="Common",profile_name="/Common/dos_orna",source_ip="192.168.32.22%0"

action="Blocking",hostname="bigip1",bigip_mgmt_ip="192.168.36.157",client_ip_geo_location="N/A",client_request_uri="/short.txt",configuration_date_time="Nov
01 2012 04:39:57",context_name="/Common/vs_159",context_type="Virtual
Server",date_time="Nov 01 2012
05:01:40",device_product="ASM",device_vendor="F5",device_version="11.3.0",dos_attack_detection_mode="TPS
Increased",dos_attack_event="Attack
ongoing",dos_attack_id="3131200721",dos_attack_name="DOS L7
attack",dos_attack_tps="0
tps",dos_dropped_requests_count="487",dos_mitigation_action="Source IP-Based
Rate Limiting",errdefs_msgno="23003140",errdefs_msg_name="Application DoS
Event",severity="7",partition_name="Common",profile_name="/Common/dos_orna",source_ip=""

action="Drop",hostname="asm176.labt.ts.example.com",bigip_mgmt_ip="192.168.69.176",context_name="",date_time="Nov
08 2012 17:58:46",dest_ip="fc55::3",dest_port="80",device_product="Advanced
Firewall
Module",device_vendor="F5",device_version="11.3.0.2790.300",dos_attack_event="Attack
Sampled",dos_attack_id="3083822789",dos_attack_name="Bad TCP
checksum",errdefs_msgno="23003138",errdefs_msg_name="Network DoS
Event",severity="8",partition_name="Common",route_domain="0",source_ip="fc55::99",source_port="20",vlan="/Common/VLAN10"
```

Example of Network DoS Protection log message in the Syslog format

```
23003138 [F5@12276 action="Drop" hostname="asm176.labt.ts.example.com"
bigip_mgmt_ip="192.168.69.176" context_name="" date_time="Nov 08 2012 18:26:02"
dest_ip="fc55::3" dest_port="80" device_product="Advanced Firewall Module"
device_vendor="F5" device_version="11.3.0.2790.300" dos_attack_event="Attack
Sampled" dos_attack_id="1493601923" dos_attack_name="Bad TCP checksum"
errdefs_msgno="23003138" errdefs_msg_name="Network DoS Event" severity="8"
partition_name="Common" route_domain="0" source_ip="fc55::99" source_port="20"
vlan="/Common/VLAN10"] "Nov 08 2012
18:26:02","192.168.69.176","asm176.labt.ts.example.com","","fc55::99","fc55::3","20","80","0","/Common/VLAN10","Bad
TCP checksum","1493601923","Attack Sampled","Drop"
```

Example of Network DoS Protection log message in the Syslog F5 format
23003138 "Nov 08 2012 18:23:14","192.168.69.176","asm176.labt.ts.example.com","","fc55::99","fc55::3","20","80","0","/Common/VLAN10","Bad TCP checksum","1493601923","Attack Sampled","Drop"

Fields in Protocol Security event messages

This table lists the fields that are contained in event messages that might display in the Protocol Security logs. The fields are listed in the order in which they appear in a message in the log.

Field name and type	Example value	Description
date_time (string)	110513:11:10	Date and time the event occurred in this format: MMM DD HH:MM:SS
hostname (string)	bigip-4.pme-ds.f5.com	BIG-IP system FQDN
PSM: (string)	PME:keword	Static value keyword
protocol (string)	FTP, SMPTP, HTTP, DNS	Protocol name
ip_client (IP address)	192.168.5.10	Client source IP address
dest_ip (IP address)	192.168.3.1	Destination IP address
vs_name (string)	Common/my_vs	Reporting virtual server name and partition
policy_name (string)	My security policy	Name of the security policy reporting the violatio
violations (string)	Active mode	Violation name
virus_name (string)	<name of virus>	Virus name
management_ip_address (IP address)	192.168.1.246	BIG-IP system management IP address
unit_hostname (string)	bigip-4.pme-ds.f5.com	BIG-IP system FQDN
request_status (string)	Blocked	Action applied to the client request
dest_port (integer)	80	Protocol port number (non-negative)
src_port (integer)	80	Protocol port number (non-negative)
route_domain (integer)	1	Route domain number (non-negative)
geo_location (string)	NY, NY, USA	City, state, country location information
violation_details (string)	port/sendport 10,3,0,33,42,88	Violation description and the values passed

Protocol Security example events

This list contains examples of events you might find in the Protocol Security logs.

Example of Protocol Security log message in the ArcSight format

```
Oct 5 11:49:13 bigip-3.pme-ds.f5.com PSM:CEF:0|F5|PSM|11.3.0|Active mode|Active
mode|5|app=FTP src=10.3.1.104 spt=1394 dst=10.3.1.204 dpt=21 cs1=ftp_security
cs1Label=policy_name cs2=/Common/FTP-3 cs2Label=vs_name dvc=192.168.73.33
dvchost=bigip-3.pme-ds.f5.com act=alerted cs6=N/A cs6Label=geo_location c6a1=
c6a1Label=device_address c6a2= c6a2Label=source_address c6a3=
c6a3Label=destination_address cs3=port/sendport 10,3,0,33,7,223
cs3Label=violation_details msg=N/A

Oct 5 11:49:13 bigip-3.pme-ds.f5.com PSM:CEF:0|F5|PSM|11.3.0|FTP commands|FTP
commands|5|app=FTP src=10.3.1.104 spt=1394 dst=10.3.1.204 dpt=21 cs1=ftp_security
cs1Label=policy_name cs2=/Common/FTP-3 cs2Label=vs_name dvc=192.168.73.33
dvchost=bigip-3.pme-ds.f5.com act=alerted cs6=N/A cs6Label=geo_location c6a1=
c6a1Label=device_address c6a2= c6a2Label=source_address c6a3=
c6a3Label=destination_address cs3=nlist/mls cs3Label=violation_details msg=N/A

Oct 5 11:49:23 bigip-3.pme-ds.f5.com PSM:CEF:0|F5|PSM|11.3.0|FTP commands|FTP
commands|5|app=FTP src=10.3.1.104 spt=1394 dst=10.3.1.204 dpt=21 cs1=ftp_security
cs1Label=policy_name cs2=/Common/FTP-3 cs2Label=vs_name dvc=192.168.73.33
dvchost=bigip-3.pme-ds.f5.com act=alerted cs6=N/A cs6Label=geo_location c6a1=
c6a1Label=device_address c6a2= c6a2Label=source_address c6a3=
c6a3Label=destination_address cs3=pwd cs3Label=violation_details msg=N/A
```

Example of Protocol Security log message in the Remote Server format

```
Oct 5 11:55:18 bigip-3.pme-ds.f5.com
PSM:protocol="FTP",ip_client="10.3.1.104",dest_ip="10.3.1.204",vs_name="/Common/FTP-3",
policy_name="ftp_security",violations="Active mode",virus_name="N/A",
management_ip_address="192.168.73.33",unit_hostname="bigip-3.pme-ds.f5.com",
request_status="alerted",dest_port="21",src_port="1397",route_domain="0",geo_location="N/A",
violation_details="port/sendport 10,3,0,33,42,88"

Oct 5 11:55:18 bigip-3.pme-ds.f5.com
PSM:protocol="FTP",ip_client="10.3.1.104",dest_ip="10.3.1.204",vs_name="/Common/FTP-3",
policy_name="ftp_security",violations="FTP commands",virus_name="N/A",
management_ip_address="192.168.73.33",unit_hostname="bigip-3.pme-ds.f5.com",
request_status="alerted",dest_port="21",src_port="1397",route_domain="0",geo_location="N/A",
violation_details="list/dir/mdir"

Oct 5 11:55:23 bigip-3.pme-ds.f5.com
PSM:protocol="FTP",ip_client="10.3.1.104",dest_ip="10.3.1.204",vs_name="/Common/FTP-3",
policy_name="ftp_security",violations="FTP commands",virus_name="N/A",
management_ip_address="192.168.73.33",unit_hostname="bigip-3.pme-ds.f5.com",
request_status="alerted",dest_port="21",src_port="1397",route_domain="0",geo_location="N/A",
violation_details="pwd"
```

Example of Protocol Security log message in the Syslog format

```
Oct 5 11:37:14 bigip-3.pme-ds.f5.com
PSM:"FTP","10.3.1.104","10.3.1.204","/Common/FTP-3","ftp_security","Active
mode","N/A","192.168.73.33","bigip-3.pme-ds.f5.com","alerted","21","1355","0","N/A","port/sendport
10,3,0,33,42,22"

Oct 5 11:37:14 bigip-3.pme-ds.f5.com
PSM:"FTP","10.3.1.104","10.3.1.204","/Common/FTP-3","ftp_security","FTP
commands","N/A","192.168.73.33","bigip-3.pme-ds.f5.com","alerted","21","1355","0","N/A","nlist/mls"
```

Example of Protocol Security log message in the Syslog format

```
Oct 5 11:37:23 bigip-3.pme-ds.f5.com
PSM:"FTP","10.3.1.104","10.3.1.204","/Common/FTP-3","ftp_security","FTP
commands","N/A","192.168.73.33","bigip-3.pme-ds.f5.com","alerted","21","1355","0","N/A","cwd
.."
```

Example of Protocol Security log message in the Syslog BSD format

```
Oct 5 11:46:26 bigip-3.pme-ds.f5.com
PSM:"FTP","10.3.1.104","10.3.1.204","/Common/FTP-3","ftp_security","Active
mode","N/A","192.168.73.33","bigip-3.pme-ds.f5.com","alerted","21","1388","0","N/A","port/sendport
10,3,0,33,7,217"

Oct 5 11:46:26 bigip-3.pme-ds.f5.com
PSM:"FTP","10.3.1.104","10.3.1.204","/Common/FTP-3","ftp_security","FTP
commands","N/A","192.168.73.33","bigip-3.pme-ds.f5.com","alerted","21","1388","0","N/A","nlist/mls"
```

Example of Protocol Security log message in the Syslog legacy format

```
Oct 5 11:43:01 bigip-3.pme-ds.f5.com
PSM:"FTP","10.3.1.104","10.3.1.204","/Common/FTP-3","ftp_security","Active
mode","N/A","192.168.73.33","bigip-3.pme-ds.f5.com","alerted","21","1370","0","N/A","port/sendport
10,3,0,33,7,197"

Oct 5 11:43:01 bigip-3.pme-ds.f5.com
PSM:"FTP","10.3.1.104","10.3.1.204","/Common/FTP-3","ftp_security","FTP
commands","N/A","192.168.73.33","bigip-3.pme-ds.f5.com","alerted","21","1370","0","N/A","nlist/mls"
```

Fields in DNS event messages

This table lists the fields that are contained in event messages that might display in the DNS logs. The fields are listed in the order in which they appear in a message in the log.

Field name and type	Example value	Description
errdefs_msgno (integer)	23003141	Static number 23003141
date_time (string)	11 13 2012 12:12:10	Date and time the event occurred in this format: MMM DD YYYY HH:MM:SS
bigip_mgmt_ip (IP address)	`192.168.1.246`	BIG-IP system management IP address
hostname (string)	`bigip-4.pme-ds.f5.com`	BIG-IP system FQDN
context_name (string)	`/Common/vs1_udp`	Partition in which the virtual server resides and name of virtual server
vlan (string)	External	Name of the VLAN interface
query_type (string)	A	Type of DNS query causing the attack
dns_query_name (string)	`siterequest.com`	Name being queried
partition_name (string)	Common	Name of the partition in which the virtual server resides
attack_type (string)	CNAME	DNS query causing the attack

Field name and type	Example value	Description
action (string)	None, Drop, Allow	Action performed or reported
src_ip (IP address)	192.168.3.1	Source IP address
dest_ip (IP address)	192.168.3.2	Destination IP address
src_port (integer)	80	Protocol port number (non-negative)
dest_port (integer)	80	Protocol port number (non-negative)
route_domain (integer)	1	Route domain number (non-negative)

DNS attack types

This table lists DNS attack types and provides a short description and classification. The attack types are listed in alphabetical order by attack name. These attacks are the DNS queries that a client can request. If the requests are received at a high rate and exceed the configured watermark they generate a DNS DoS event

Attack name (RFC number)	Description
a6 (1035)	Returns a 32-bit IPv4 IP address record
aaaa (3596)	Returns a 128-bit IPv6 address record
afsdb (1183)	Location of database servers of an AFS database record record
any (1035)	Returns all cached records of all types
atma	ATM address
axfr (1035)	Authoritative zone transfer
cert (4398)	Stores PKIX, SPKI, and PGP certificate record
cname (1035)	Alias of one name to another (canonical name record)
dname (2672)	DNAME (delegation name) creates an alias for a name and all its subnames
eid	Endpoint identifier
gpos (1712)	Geographical position (state, country)
hinfo (1035)	Host information
isdn (1183)	ISDN address
ixfr (1996)	Incrementatl zone transfer
key (2535, 2930)	Used only for SIG(0) (RFC 2931) and TKEY (RFC 2930).[5] key records
kx (2535, 2930)	Key exchange record identifies a key management agent for the associated domain-name (not associated with DNSSEC)
loc (1876)	Location record
maila (1035)	Request for mail agent resource records
mailb (1035)	Mailbox or mail list information (MINFO)
mb (1035)	Mailbox domain name

Attack name (RFC number)	Description
md	Mail destination
mf (1035)	Mail forwarder
mg (1035)	Mail group member
minfo (1035)	Mailbox or mail list information
mr (1035)	Mail rename domain name
mx (1035)	Mail exchange record
naptr (3403)	Naming authority pointer
nimloc (1002)	Nimrod locator
ns (1035)	Nameserver record
nsap (1706)	NSAP style A record
nsap-ptr (1348)	NSAP style domain name pointer
null (1035)	Null resource record
nxt (2535)	Next domain
opt (2671)	Pseudo DNS record type that supports EDNS
ptr (1035)	Pointer to a canonical name
px (2163)	X.400 mail mapping information
rp (1183)	Contact information for the person(s) responsible for the domain
rt (1183)	Route through
sg (2535)	Signature record
sink	DNS sinkhole
soa (1035)	Start of authority record
srv (2782)	Service locator record
tkey (2930)	Secret key record
tsig (2845)	Transaction signature that authenticates dynamic updates as coming from an approved client, or authenticates responses as coming from an approved recursive name server
txt (1035)	Text record
wks	Sender Policy Framework, DKIM, and DMARC DNS-SD
x25 (1183)	X.25 PSDN address
zxfr	Compressed zone transfer

DNS example events

This list contains examples of events you might find in the DNS logs.

Example of DNS log message in the ArcSight CEF format

```
Oct 12 13:35:47 10.3.0.33 CEF:0|F5|Advanced Firewall
Module|11.3.0.2206.0|23003139|DNS Event|8|rt=Oct 12 2012 13:29:24
dvchost=bigip-3.pme-ds.f5.com dvc=192.68.73.33 src=10.3.1.104 spt=54629
dst=10.3.1.202 dpt=53 cs1=/Common/DNS-3-udp-vs cs1Label=virtual_name
cs2=/Common/external cs2Label=vlan cs3=SRV cs3Label=query_type act=Drop
cs4=_ldap._tcp.dc._msdcs.siterequest.com cs4Label=query_name cs5=query opcode
cs5Label=attack_type c6a2= c6a2Label=source_address c6a3=
c6a3Label=destination_address
```

Example of DNS log message in the Reporting Server format

```
"Oct 26 2012
06:23:13","192.168.69.245","asm245.labt.ts.example.com","/Common/vs2_udp","
/Common/vlan1","A","domain1.local","A","Drop","10.10.10.2","10.10.10.251","4000","53","0"
```

Example of DNS log message in the Syslog format

```
"Oct 26 2012
06:23:13","192.168.69.245","asm245.labt.ts.example.com","/Common/vs2_udp","
/Common/vlan1","A","domain1.local","A","Drop","10.10.10.2","10.10.10.251","4000","53","0"
```

Fields in DNS DoS event messages

This table lists the fields that are contained in event messages that might display in the Network DNS DoS logs. The fields are listed in the order in which they appear in a message in the log.

Field name and type	Example value	Description
errdefs_msgno (integer)	23003141	Static number
errdefs_msg_name (string)	DNS DoS Event	Name of event
date_time (string)	11 13 2012 12:12:10	Date and time event occurred in this format: MMM DD YYYY HH:MM:SS
bigip_mgmt_ip (IP address)	192.168.1.246	BIG-IP system management IP address
hostname (string)	`bigip-4.pme-ds.f5.com`	BIG-IP system FQDN
context_name (string)	`/Common/vs1_udp`	Partition in which the virtual server resides and name of virtual server
vlan (string)	External	Name of VLAN interface
dns_query_type (string)	A	Type of DNS query causing the attack
dns_query_name (string)	`f5.com`	Name being queried
src_ip (IP address)	`192.168.3.1`	Source IP address
dest_ip (IP address)	`192.168.3.1`	Destination IP address
src_port (integer)	80	Protocol port number (non-negative)
dest_port (integer)	80	Protocol port number (non-negative)
partition_name (string)	Common	Name of the partition in which the virtual server resides

Field name and type	Example value	Description
dos_attack_name (string)	A query DOS	Name of attack
dos_attack_id (integer)	1005891899	Unique, non-negative, attack instance ID
dos_attack_event (string)	Attack Sampled	Status of attack
action (string)	None, Drop, Allow	Action performed or reported

DNS DoS attack types

This table lists DNS DoS attack types and provides a short description and classification. The attack types are listed in alphabetical order by attack name.

Attack name (RFC)	Description	Value description
A query DOS (RFC 1035)	Returns a 32-bit IPv4 address, most commonly used to map hostnames to an IP address of the host, but also used for DNSBLs, storing subnet masks in RFC 1101.	Address record
PTR query DOS (RFC 1035)	Pointer to a canonical name. Unlike a CNAME, DNS processing does not proceed, and only the name is returned. The most common use is for implementing reverse DNS lookups, but other uses include such things as DNS-SD.	Pointer record
NS query DOS (1035)	Delegates a DNS zone to use the given authoritative name servers.	Name service record
SOA query DOS (1035)	Specifies authoritative information about a DNS zone, including the primary name server, the email of the domain administrator, the domain serial number, and several timers relating to refreshing the zone.	Start of authority record
CNAME query DOS (1035)	Alias of one name to another: the DNS lookup will continue by retrying the lookup with the new name.	Canonical name record
MX query DOS (1035)	Maps a domain name to a list of message transfer agents for that domain.	Mail exchange record
AAAA query DOS (3596)	Returns a 128-bit IPv6 address, most commonly used to map hostnames to an IP address of the host.	IPv6 address record
TXT query DOS (1035)	Originally for arbitrary human-readable text in a DNS record, however, this record often carries machine-readable data, such as specified by RFC 1464, opportunistic encryption, Sender Policy Framework, DKIM, and DMARC DNS-SD.	Text record
SRV query DOS (2782)	Generalized service location record, used for newer protocols instead of creating protocol-specific records such as MX.	Service locator
AXFR query DOS (1035)	Request for a transfer of an entire zone.	Request
IXFR query DOS (1995)	Incremental transfer of records in the zone.	Request
ANY query DOS (1035)	Request for all records.	Request

Attack name (RFC)	Description	Value description
Malformed DOS	Generated by a DNS packet in which one of the fields, for example, opcode, query_type or query_name, contains invalid information.	
Malicious DOS	Generated by malicious packets, that is, malformed DNS packets with references that are invalid.	
Other Query DOS	Queries, not listed in this table, which are being used to attack nameservers.	

DNS DoS example events

This list contains examples of events you might find in the DNS DoS attack logs.

Example of DNS DoS attack log message in the Syslog format
"Oct 30 2012 10:57:09","192.168.56.179","Surya_BIG_IP_VM1.example.com","/Common/vs_192_168_57_177_53_gtm","/Common/external","A","surya.example.com","192.168.56.171","192.168.57.177","43835","53","0","A query DOS","1005891899","Attack Sampled","Allow"

BIG-IP system process example events

This list contains examples of events you might find in BIG-IP system logs. Please be aware that system log messages might be truncated, because the UDP protocol cannot send large messages. Note that using the TCP protocol impacts performance.

Example Syslog log entry for the system audit log

This log entry provides confirmation of a successful configuration save.

```
1 2012-11-01T18:07:13Z bigip-3.pme-ds.f5.com tmsh 29639 01420002:5:
[F5@12276 hostname="bigip-3.pme-ds.f5.com" errdefs_msgno="01420002:5:"]
AUDIT - pid=29639 user=root folder=/Common module=(tmos)#
status=[Command OK] cmd_data=save / sys config partitions all
```

Example Syslog log entry for the application security log

This log entry provides confirmation of the end of a DoS attack.

```
Nov 01 14:15:44 10.3.0.33 1 2012-11-01T18:09:38Z bigip-3.pme-ds.f5.com
2 28965 01010253:5: [F5@12276 hostname="bigip-3.pme-ds.f5.com"
errdefs_msgno="01010253:5:"] A DOS attack has stopped for vector Ethernet
broadcast packet, Attack ID 188335952.
```

IPFIX Templates for CGNAT Events

Overview: IPFIX logging templates

The IP Flow Information Export (IPFIX) Protocol is a logging mechanism for IP events. This appendix defines the IPFIX information elements (IEs) and templates used to log the F5 CGNAT events. An *IE* is the smallest form of useful information in an IPFIX log message, such as an IP address or a timestamp for the event. An *IPFIX template* is an ordered collection of specific IEs used to record one IP event, such as the establishment of an inbound NAT64 session.

IPFIX information elements for CGNAT events

Information elements (IEs) are individual fields in an IPFIX template. An IPFIX template describes a single CGNAT event. These tables list all the IEs used in F5 CGNAT events, and differentiate IEs defined by IANA from IEs defined by F5 products.

IANA-Defined IPFIX information elements

Information Elements

IANA maintains a list of standard IPFIX information elements (IEs), each with a unique element identifier, at *http://www.iana.org/assignments/ipfix/ipfix.xml*. The F5 CGNAT implementation uses a subset of these IEs to publish CGNAT events. This subset is summarized in the table below. Please refer to the IANA site for the official description of each field.

Information Element (IE)	ID	Size (Bytes)
destinationIPv4Address	12	4
destinationTransportPort	11	2
egressVRFID	235	4
flowDurationMilliseconds	161	4
flowStartMilliseconds	152	8
ingressVRFID	234	4
natEvent	230	1
natOriginatingAddressRealm	229	1
natPoolName	284	Variable
observationTimeMilliseconds	323	8
portRangeEnd	362	2
portRangeStart	361	2

Information Element (IE)	ID	Size (Bytes)
postNAPTDestinationTransportPort	228	2
postNAPTSourceTransportPort	227	2
postNATDestinationIPv4Address	226	4
postNATDestinationIPv6Address	282	16
postNATSourceIPv4Address	225	4
protocolIdentifier	4	1
sourceIPv4Address	8	4
sourceIPv6Address	27	16
sourceTransportPort	7	2

Note: *IPFIX, unlike NetFlow v9, supports variable-length IEs, where the length is encoded within the field in the Data Record. NetFlow v9 collectors (and their variants) cannot correctly process variable-length IEs, so they are omitted from logs sent to those collector types.*

IPFIX enterprise information elements

Description

IPFIX provides specifications for enterprises to define their own Information Elements. F5 currently does not use any non-standard IEs for CGNAT Events.

Individual IPFIX templates for each event

These tables specify the IPFIX templates used by F5 to publish CGNAT Events.

Each template contains a *natEvent* information element (IE). This element is currently defined by IANA to contain values of 1 (Create Event), 2 (Delete Event) and 3 (Pool Exhausted). In the future, it is possible that IANA will standardize additional values to distinguish between NAT44 and NAT64 events, and to allow for additional types of NAT events. For example, the *http://datatracker.ietf.org/doc/draft-ietf-behave-ipfix-nat-logging* Internet Draft proposes additional values for this IE for such events.

F5 uses the standard Create and Delete *natEvent* values in its IPFIX Data Records, rather than new (non-standard) specific values for NAT44 Create, NAT64 Create, and so on.

You can infer the semantics of each template (for example, whether or not the template applies to NAT44 Create, NAT64 Create, or DS-Lite Create) from the template's contents rather than from distinct values in the natEvent IE.

F5 CGNAT might generate different variants of NAT Session Create/Delete events, to cater to customer requirements such as the need to publish destination address information, or to specifically omit such information. Each variant has a distinct template.

The “Pool Exhausted” *natEvent* value is insufficiently descriptive to cover the possible NAT failure cases. Therefore, pending future updates to the *natEvent* Information Element, F5 uses some non-standard values to cover the following cases:

- 10 – Translation Failure
- 11 – Session Quota Exceeded
- 12 – Port Quota Exceeded
- 13 - Port Block Allocated
- 14 - Port Block Released
- 15 - Port Block Allocation (PBA) Client Block Limit Exceeded
- 16 - PBA Port Quota Exceeded

The following tables enumerate and define the IPFIX templates, and include the possible *natEvent* values for each template.

NAT44 session create – outbound variant

Description

This event is generated when a NAT44 client session is received from the subscriber side and the LSN process successfully translates the source address/port.

Information Element (IE)	ID	Size (Bytes)	Notes
observationTimeMilliseconds	323	8	
ingressVRFID	234	4	The "client" routing-domain ID.
egressVRFID	235	4	The "LSN" routing-domain ID.
sourceIPv4Address	8	4	
postNATSourceIPv4Address	225	4	
protocolIdentifier	4	1	
sourceTransportPort	7	2	
postNAPTSourceTransportPort	227	2	
destinationIPv4Address	12	4	0 (zero) if obscured.
destinationTransportPort	11	2	0 (zero) if obscured.
natOriginatingAddressRealm	229	1	1 (private/internal realm, subscriber side).
natEvent	230	1	1 (for Create event).

NAT44 session delete – outbound variant

Description

This event is generated when a NAT44 client session is received from the subscriber side and the LSN process finishes the session.

By default, the BIG-IP® system does not record "delete session" events like this one. This default exists to improve performance, but it prevents the system from ever sending IPFIX logs matching this template. To enable "delete session" events and IPFIX logs matching this template, use the following `tmsh` command:

```
modify sys db log.lsn.session.end value enable
```

Information Element (IE)	ID	Size (Bytes)	Notes
observationTimeMilliseconds	323	8	
ingressVRFID	234	4	The "client" routing-domain ID.
egressVRFID	235	4	The "LSN" routing-domain ID.
sourceIPv4Address	8	4	
postNATSourceIPv4Address	225	4	
protocolIdentifier	4	1	
sourceTransportPort	7	2	
postNAPTSourceTransportPort	227	2	
destinationIPv4Address	12	4	0 (zero) if obscured.
destinationTransportPort	11	2	0 (zero) if obscured.
natOriginatingAddressRealm	229	1	1 (private/internal realm, subscriber side).
natEvent	230	1	2 (for Delete event).
flowStartMilliseconds	152	8	Start time, in ms since Epoch (1/1/1970).
flowDurationMilliseconds	161	4	Duration in ms.

NAT44 session create – inbound variant

Description

This event is generated when an inbound NAT44 client session is received from the internet side and connects to a client on the subscriber side.

Information Element (IE)	ID	Size (Bytes)	Notes
observationTimeMilliseconds	323	8	
ingressVRFID	234	4	The "LSN" routing-domain ID.
egressVRFID	235	4	The "client" routing-domain ID.
sourceIPv4Address	8	4	
protocolIdentifier	4	1	
sourceTransportPort	7	2	
destinationIPv4Address	12	4	
postNATDestinationIPv4Address	226	4	

Information Element (IE)	ID	Size (Bytes)	Notes
destinationTransportPort	11	2	
postNAPTDestinationTransportPort	228	2	
natOriginatingAddressRealm	229	1	2 (public/external realm, Internet side).
natEvent	230	1	1 (for Create event).

NAT44 session delete – inbound variant

Description

This event is generated when an inbound NAT44 client session is received from the internet side and connects to a client on the subscriber side. This event is the deletion of the inbound connection.

By default, the BIG-IP® system does not record "delete session" events like this one. This default exists to improve performance, but it prevents the system from ever sending IPFIX logs matching this template. To enable "delete session" events and IPFIX logs matching this template, use the following `tmsh` command:

```
modify sys db log.lsn.session.end value enable
```

Information Element (IE)	ID	Size (Bytes)	Notes
observationTimeMilliseconds	323	8	
ingressVRFID	234	4	The "LSN" routing-domain ID.
egressVRFID	235	4	The "client" routing-domain ID.
sourceIPv4Address	8	4	
protocolIdentifier	4	1	
sourceTransportPort	7	2	
destinationIPv4Address	12	4	
postNATDestinationIPv4Address	226	4	
destinationTransportPort	11	2	
postNAPTDestinationTransportPort	228	2	
natOriginatingAddressRealm	229	1	2 (public/external realm, Internet side).
natEvent	230	1	2 (for Delete event).
flowStartMilliseconds	152	8	Start time, in ms since Epoch (1/1/1970).
flowDurationMilliseconds	161	4	Duration in ms.

NAT44 translation failed

Description

This event reports a NAT44 Translation Failure. The failure does not necessarily mean that all addresses or ports in the translation pool are already in use; the implementation may not be able to find a valid translation within the allowed time constraints or number of lookup attempts, as may happen if the pool has become highly fragmented.

Information Element (IE)	ID	Size (Bytes)	Notes
observationTimeMilliseconds	323	8	
ingressVRFID	234	4	The "client" routing-domain ID.
sourceIPv4Address	8	4	
protocolIdentifier	4	1	
sourceTransportPort	7	2	
destinationIPv4Address	12	4	0 (zero) if obscured.
destinationTransportPort	11	2	0 (zero) if obscured.
natEvent	230	1	10 for Transmission Failed.
natPoolName	284	Variable	This IE is omitted for NetFlow v9.

NAT44 quota exceeded

Description

This event is generated when an administratively configured policy prevents a successful NAT44 translation.

Information Element (IE)	ID	Size (Bytes)	Notes
observationTimeMilliseconds	323	8	
ingressVRFID	234	4	The "client" routing-domain ID.
sourceIPv4Address	8	4	
natEvent	230	1	11 for Session Quota Exceeded, 12 for Port Quota Exceeded, 15 for PBA client block limit Exceeded, 16 for PBA Port Quota Exceeded.
natPoolName	284	Variable	This IE is omitted for NetFlow v9.

NAT44 port block allocated or released

Description

This event is generated when the BIG-IP software allocates or releases a block of ports for a NAT44 client. The event only occurs when port-block allocation (PBA) is configured for the LSN pool. When an LSN pool uses PBA, it only issues an IPFIX log for every block of CGNAT translations. This reduces IPFIX traffic for CGNAT.

Information Element (IE)	ID	Size (Bytes)	Notes
observationTimeMilliseconds	323	8	
ingressVRFID	234	4	The "client" routing-domain ID.
egressVRFID	235	4	The egress routing-domain ID.
sourceIPv4Address	8	4	
postNATSourceIPv4Address	225	4	
portRangeStart	361	2	
portRangeEnd	362	2	
natEvent	230	1	13 for PBA, block Allocated, 14 for PBA, block released.

NAT64 session create – outbound variant

Description

This event is generated when a NAT64 client session is received from the subscriber side and the LSN process successfully translates the source address/port.

Note: *The* `destinationIPv6Address` *is not reported, since the* `postNATdestinationIPv4Address` *value is derived algorithmically from the IPv6 representation in* `destinationIPv6Address`*, as specified in RFC 6146 and RFC 6502.*

Information Element (IE)	ID	Size (Bytes)	Notes
observationTimeMilliseconds	323	8	
ingressVRFID	234	4	The "client" routing-domain ID.
egressVRFID	235	4	The "LSN" routing-domain ID.
sourceIPv6Address	27	16	
postNATSourceIPv4Address	225	4	
protocolIdentifier	4	1	
sourceTransportPort	7	2	
postNAPTSourceTransportPort	227	2	
postNATDestinationIPv4Address	226	4	0 (zero) if obscured.

Information Element (IE)	ID	Size (Bytes)	Notes
destinationTransportPort	11	2	0 (zero) if obscured.
natOriginatingAddressRealm	229	1	1 (private/internal realm, subscriber side).
natEvent	230	1	1 (for Create event).

NAT64 session delete – outbound variant

Description

This event is generated when a NAT64 client session is received from the subscriber side and the LSN process finishes the outbound session.

By default, the BIG-IP® system does not record "delete session" events like this one. This default exists to improve performance, but it prevents the system from ever sending IPFIX logs matching this template. To enable "delete session" events and IPFIX logs matching this template, use the following `tmsh` command:

```
modify sys db log.lsn.session.end value enable
```

Information Element (IE)	ID	Size (Bytes)	Notes
observationTimeMilliseconds	323	8	
ingressVRFID	234	4	The "client" routing-domain ID.
egressVRFID	235	4	The "LSN" routing-domain ID.
sourceIPv6Address	27	16	
postNATSourceIPv4Address	225	4	
protocolIdentifier	4	1	
sourceTransportPort	7	2	
postNAPTSourceTransportPort	227	2	
postNATDestinationIPv4Address	226	4	0 (zero) if obscured.
destinationTransportPort	11	2	0 (zero) if obscured.
natOriginatingAddressRealm	229	1	1 (private/internal realm, subscriber side).
natEvent	230	1	2 (for Delete event).
flowStartMilliseconds	152	8	Start time, in ms since Epoch (1/1/1970).
flowDurationMilliseconds	161	4	Duration in ms.

NAT64 session create – inbound variant

Description

This event is generated when a client session comes in from the internet side and successfully connects to a NAT64 client on the subscriber side.

Note: *`postNATSourceIPv6Address` is not reported since this value can be derived algorithmically from by appending the well-known NAT64 prefix 64:ff9b:: to `sourceIPv4Address`.*

Information Element (IE)	ID	Size (Bytes)	Notes
observationTimeMilliseconds	323	8	
ingressVRFID	234	4	The "LSN" routing-domain ID.
egressVRFID	235	4	The "client" routing-domain ID.
sourceIPv4Address	8	4	
protocolIdentifier	4	1	
sourceTransportPort	7	2	
destinationIPv4Address	12	4	
postNATDestinationIPv6Address	282	16	
destinationTransportPort	11	2	
postNAPTDestinationTransportPort	228	2	
natOriginatingAddressRealm	229	1	2 (public/external realm, Internet side).
natEvent	230	1	1 (for Create event).

NAT64 session delete – inbound variant

Description

This event is generated when a client session comes in from the internet side and successfully connects to a NAT64 client on the subscriber side. This event is the deletion of the inbound connection.

Note: *`postNATSourceIPv6Address` is not reported since this value can be derived algorithmically from by appending the well-known NAT64 prefix 64:ff9b:: to `sourceIPv4Address`.*

By default, the BIG-IP® system does not record "delete session" events like this one. This default exists to improve performance, but it prevents the system from ever sending IPFIX logs matching this template. To enable "delete session" events and IPFIX logs matching this template, use the following `tmsh` command:

```
modify sys db log.lsn.session.end value enable
```

Information Element (IE)	ID	Size (Bytes)	Notes
observationTimeMilliseconds	323	8	

Information Element (IE)	ID	Size (Bytes)	Notes
ingressVRFID	234	4	The "LSN" routing-domain ID.
egressVRFID	235	4	The "client" routing-domain ID.
sourceIPv4Address	8	4	
protocolIdentifier	4	1	
sourceTransportPort	7	2	
destinationIPv4Address	12	4	
postNATDestinationIPv6Address	282	16	
destinationTransportPort	11	2	
postNAPTDestinationTransportPort	228	2	
natOriginatingAddressRealm	229	1	2 (public/external realm, Internet side).
natEvent	230	1	2 (for Delete event).
flowStartMilliseconds	152	8	Start time, in ms since Epoch (1/1/1970).
flowDurationMilliseconds	161	4	Duration in ms.

NAT64 translation failed

Description

This event reports a NAT64 Translation Failure. The failure does not necessarily mean that all addresses or ports in the translation pool are already in use; the implementation may not be able to find a valid translation within the allowed time constraints or number of lookup attempts, as may happen if the pool has become highly fragmented.

Information Element (IE)	ID	Size (Bytes)	Notes
observationTimeMilliseconds	323	8	
ingressVRFID	234	4	The "client" routing-domain ID.
sourceIPv6Address	27	16	
protocolIdentifier	4	1	
sourceTransportPort	7	2	
destinationIPv4Address	12	4	0 (zero) if obscured.
destinationTransportPort	11	2	0 (zero) if obscured.
natEvent	230	1	10 for Transmission Failed.
natPoolName	284	Variable	This IE is omitted for NetFlow v9.

NAT64 quota exceeded

Description

This event is generated when an administratively configured policy prevents a successful NAT64 translation.

Information Element (IE)	ID	Size (Bytes)	Notes
observationTimeMilliseconds	323	8	
ingressVRFID	234	4	The "client" routing-domain ID.
sourceIPv6Address	27	16	
natEvent	230	1	11 for Session Quota Exceeded, 12 for Port Quota Exceeded, 15 for PBA client block limit Exceeded, 16 for PBA Port Quota Exceeded.
natPoolName	284	Variable	This IE is omitted for NetFlow v9.

NAT64 port block allocated or released

Description

This event is generated when the BIG-IP software allocates or releases a block of ports for a NAT64 client. The event only occurs when port-block allocation (PBA) is configured for the LSN pool. When an LSN pool uses PBA, it only issues an IPFIX log for every block of CGNAT translations. This reduces IPFIX traffic for CGNAT.

Information Element (IE)	ID	Size (Bytes)	Notes
observationTimeMilliseconds	323	8	
ingressVRFID	234	4	The "client" routing-domain ID.
egressVRFID	235	4	The egress routing-domain ID.
sourceIPv6Address	27	16	
postNATSourceIPv4Address	225	4	
portRangeStart	361	2	
portRangeEnd	362	2	
natEvent	230	1	13 for PBA, block Allocated, 14 for PBA, block released.

DS-Lite session create – outbound variant

Description

This event is generated when a DS-Lite client session is received on the subscriber side and the LSN process successfully translates the source address/port. The client's DS-Lite IPv6 remote endpoint address is reported using IE `lsnDsLiteRemoteV6asSource`.

Note: *The `sourceIPv6Address` stores different information in this template from the equivalent NAT64 template. In the NAT64 create and delete templates, `sourceIPv6Address` holds the client's IPv6 address. In this DS-Lite template, it holds the remote endpoint address of the DS-Lite tunnel.*

Note: *The VRFID (or routing domain ID) for the DS-Lite tunnel is not currently provided; this attribute may be added in the future.*

Information Element (IE)	ID	Size (Bytes)	Notes
observationTimeMilliseconds	323	8	
ingressVRFID	234	4	The "client" routing-domain ID.
egressVRFID	235	4	The "LSN" routing-domain ID.
sourceIPv4Address	8	4	
postNATSourceIPv4Address	225	4	
protocolIdentifier	4	1	
sourceTransportPort	7	2	
postNAPTSourceTransportPort	227	2	
sourceIPv6Address	27	16	DS-Lite remote endpoint IPv6 address.
destinationIPv4Address	12	4	0 (zero) if obscured.
destinationTransportPort	11	2	0 (zero) if obscured.
natOriginatingAddressRealm	229	1	1 (private/internal realm, subscriber side).
natEvent	230	1	1 (for Create event).

DS-Lite session delete – outbound variant

Description

This event is generated when a DS-Lite client session is received from the subscriber side and the LSN process finishes with the outbound session.

Note: *The `sourceIPv6Address` stores different information in this template from the equivalent NAT64 template. In the NAT64 create and delete templates, `sourceIPv6Address` holds the client's IPv6 address. In this DS-Lite template, it holds the remote endpoint address of the DS-Lite tunnel.*

Note: *The VRFID (or routing domain ID) for the DS-Lite tunnel is not currently provided; this attribute may be added in the future.*

By default, the BIG-IP® system does not record "delete session" events like this one. This default exists to improve performance, but it prevents the system from ever sending IPFIX logs matching this template. To enable "delete session" events and IPFIX logs matching this template, use the following `tmsh` command:

```
modify sys db log.lsn.session.end value enable
```

Information Element (IE)	ID	Size (Bytes)	Notes
observationTimeMilliseconds	323	8	
ingressVRFID	234	4	The "client" routing-domain ID.
egressVRFID	235	4	The "LSN" routing-domain ID.
sourceIPv4Address	8	4	
postNATSourceIPv4Address	225	4	
protocolIdentifier	4	1	
sourceTransportPort	7	2	
postNAPTSourceTransportPort	227	2	
sourceIPv6Address	27	16	DS-Lite remote endpoint IPv6 address.
destinationIPv4Address	12	4	0 (zero) if obscured.
destinationTransportPort	11	2	0 (zero) if obscured.
natOriginatingAddressRealm	229	1	1 (private/internal realm, subscriber side).
natEvent	230	1	2 (for Delete event).
flowStartMilliseconds	152	8	Start time, in ms since Epoch (1/1/1970).
flowDurationMilliseconds	161	4	Duration in ms.

DS-Lite session create – inbound variant

Description

This event is generated when an inbound client session comes in from the internet side and connects to a DS-Lite client on the subscriber side.

Information Element (IE)	ID	Size (Bytes)	Notes
observationTimeMilliseconds	323	8	
ingressVRFID	234	4	The "LSN" routing-domain ID.
egressVRFID	235	4	The "client" routing-domain ID.
sourceIPv4Address	8	4	
protocolIdentifier	4	1	

Information Element (IE)	ID	Size (Bytes)	Notes
sourceTransportPort	7	2	
destinationIPv4Address	12	4	
postNATDestinationIPv6Address	282	16	DS-Lite remote endpoint IPv6 address.
postNATDestinationIPv4Address	226	4	
destinationTransportPort	11	2	
postNAPTDestinationTransportPort	228	2	
natOriginatingAddressRealm	229	1	2 (public/external realm, Internet side).
natEvent	230	1	1 (for Create event).

DS-Lite session delete – inbound variant

Description

This event is generated when an inbound client session comes in from the internet side and connects to a DS-Lite client on the subscriber side. This event marks the end of the inbound connection, when the connection is deleted.

By default, the BIG-IP® system does not record "delete session" events like this one. This default exists to improve performance, but it prevents the system from ever sending IPFIX logs matching this template. To enable "delete session" events and IPFIX logs matching this template, use the following `tmsh` command:

```
modify sys db log.lsn.session.end value enable
```

Information Element (IE)	ID	Size (Bytes)	Notes
observationTimeMilliseconds	323	8	
ingressVRFID	234	4	The "LSN" routing-domain ID.
egressVRFID	235	4	The "client" routing-domain ID.
sourceIPv4Address	8	4	
protocolIdentifier	4	1	
sourceTransportPort	7	2	
destinationIPv4Address	12	4	
postNATDestinationIPv6Address	282	16	
postNATDestinationIPv4Address	226	4	
destinationTransportPort	11	2	
postNAPTDestinationTransportPort	228	2	
natOriginatingAddressRealm	229	1	2 (public/external realm, Internet side).
natEvent	230	1	2 (for Delete event).
flowStartMilliseconds	152	8	Start time, in ms since Epoch (1/1/1970).

Information Element (IE)	ID	Size (Bytes)	Notes
flowDurationMilliseconds	161	4	Duration in ms.

DS-Lite translation failed

Description

This event reports a DS-Lite Translation Failure. The failure does not necessarily mean that all addresses or ports in the translation pool are already in use; the implementation may not be able to find a valid translation within the allowed time constraints or number of lookup attempts, as may happen if the pool has become highly fragmented.

Information Element (IE)	ID	Size (Bytes)	Notes
observationTimeMilliseconds	323	8	
ingressVRFID	234	4	The "client" routing-domain ID.
sourceIPv4Address	8	4	IPv4 address used by F5 CGNAT in the IPv4-mapped IPv6 format, for the DS-Lite tunnel terminated on the BIG-IP.
protocolIdentifier	4	1	
sourceTransportPort	7	2	
sourceIPv6Address	27	16	IPv6 address for remote endpoint of the DS-Lite tunnel.
destinationIPv4Address	12	4	0 (zero) if obscured.
destinationTransportPort	11	2	0 (zero) if obscured.
natEvent	230	1	10 for Transmission Failed.
natPoolName	284	Variable	This IE is omitted for NetFlow v9.

DS-Lite quota exceeded

Description

This event is generated when an administratively configured policy prevents a successful NAT translation in a DS-Lite context.

Information Element (IE)	ID	Size (Bytes)	Notes
observationTimeMilliseconds	323	8	
ingressVRFID	234	4	The "client" routing-domain ID.
sourceIPv4Address	8	4	
sourceIPv6Address	27	16	DS-Lite remote endpoint IPv6 address.
natEvent	230	1	11 for Session Quota Exceeded, 12 for Port Quota Exceeded, 15 for PBA client

Information Element (IE)	ID	Size (Bytes)	Notes
			block limit Exceeded, 16 for PBA Port Quota Exceeded.
natPoolName	284	Variable	This IE is omitted for NetFlow v9.

DS-Lite port block allocated or released

Description

This event is generated when the BIG-IP software allocates or releases a block of ports for a DS-Lite client. This event only occurs when port-block allocation (PBA) is configured for the LSN pool. When an LSN pool uses PBA, it issues an IPFIX log for every block of CGNAT translations rather than each individual translation. This reduces IPFIX traffic for CGNAT.

Information Element (IE)	ID	Size (Bytes)	Notes
observationTimeMilliseconds	323	8	
ingressVRFID	234	4	The "client" routing-domain ID.
egressVRFID	235	4	The egress routing-domain ID.
sourceIPv6Address	27	16	
postNATSourceIPv4Address	225	4	
portRangeStart	361	2	
portRangeEnd	362	2	
natEvent	230	1	13 for PBA, block Allocated, 14 for PBA, block released.

IPFIX Templates for AFM Events

Overview: IPFIX Templates for AFM Events

The IP Flow Information Export (IPFIX) Protocol is a logging mechanism for IP events. This appendix defines the IPFIX Information Elements (IEs) and Templates used to log F5's Application Firewall Manager (AFM) events. An *IE* is the smallest form of useful information in an IPFIX log message, such as an IP address or a timestamp for the event. An *IPFIX template* is an ordered collection of specific IEs used to record one IP event, such as the acceptance of a network packet.

About IPFIX Information Elements for AFM events

Information Elements (IEs) are individual fields in an IPFIX template. An IPFIX template describes a single Advanced Firewall Manager™(AFM™) event.

IANA-defined IPFIX Information Elements

IANA maintains a list of standard IPFIX Information Elements (IEs), each with a unique Element Identifier. The F5® AFM™ IPFIX implementation uses a subset of these IEs to publish AFM events. This subset is summarized in the table.

Information Element (IE)	ID	Size (Bytes)
destinationIPv4Address	12	4
destinationIPv6Address	28	16
destinationTransportPort	11	2
ingressVRFID	234	4
observationTimeMilliseconds	323	8
protocolIdentifier	4	1
sourceIPv4Address	8	4
sourceIPv6Address	27	16
sourceTransportPort	7	2

IPFIX enterprise Information Elements

IPFIX provides for enterprises to define their own Information Elements. F5® currently uses the following non-standard IEs for AFM™ events:

Information Element (IE)	ID	Size (Bytes)
aclPolicyName	12276 - 26	Variable
aclPolicyType	12276 - 25	Variable
aclRuleName	12276 - 38	Variable
action	12276 - 39	Variable
attackType	12276 - 46	Variable
bigipHostName	12276 - 10	Variable
bigipMgmtIPv4Address	12276 - 5	4
bigipMgmtIPv6Address	12276 - 6	16
contextName	12276 - 9	Variable
contextType	12276 - 24	Variable
destinationGeo	12276 - 43	Variable
deviceProduct	12276 - 12	Variable
deviceVendor	12276 - 11	Variable
deviceVersion	12276 - 13	Variable
dosAttackEvent	12276 - 41	Variable
dosAttackId	12276 - 20	4
dosAttackName	12276 - 21	Variable
dosPacketsDropped	12276 - 23	4
dosPacketsReceived	12276 - 22	4
dropReason	12276 - 40	Variable
errdefsMsgNo	12276 - 4	4
flowId	12276 - 3	8
ipfixMsgNo	12276 - 16	4
ipintelligencePolicyName	12276 - 45	Variable
ipintelligenceThreatName	12276 - 42	Variable
logMsgDrops	12276 - 96	4
logMsgName	12276 - 97	Variable
logprofileName	12276 - 95	Variable
messageSeverity	12276 - 1	1
msgName	12276 - 14	Variable
partitionName	12276 - 2	Variable
saTransPool	12276 - 37	Variable
saTransType	12276 - 36	Variable
sourceGeo	12276 - 44	Variable
sourceUser	12276 - 93	Variable
transDestinationIPv4Address	12276 - 31	4

Information Element (IE)	ID	Size (Bytes)
transDestinationIPv6Address	12276 - 32	16
transDestinationPort	12276 - 33	2
transIpProtocol	12276 - 27	1
transRouteDomain	12276 - 35	4
transSourceIPv4Address	12276 - 28	4
transSourceIPv6Address	12276 - 29	16
transSourcePort	12276 - 30	2
transVlanName	12276 - 34	Variable
vlanName	12276 - 15	Variable

Note: *IPFIX, unlike NetFlow v9, supports variable-length IEs, where the length is encoded within the field in the Data Record. NetFlow v9 collectors (and their variants) cannot correctly process variable-length IEs, so they are omitted from logs sent to those collector types.*

About individual IPFIX templates for each event

F5® uses IPFIX templates to publish AFM™ events.

Network accept or deny

This IPFIX template is used whenever a network packet is accepted or denied by an AFM™ firewall.

Information Element (IE)	ID	Size (Bytes)	Notes
aclPolicyName	12276 - 26	Variable	This IE is omitted for NetFlow v9.
aclPolicyType	12276 - 25	Variable	This IE is omitted for NetFlow v9.
aclRuleName	12276 - 38	Variable	This IE is omitted for NetFlow v9.
action	12276 - 39	Variable	This IE is omitted for NetFlow v9.
bigipHostName	12276 - 10	Variable	This IE is omitted for NetFlow v9.
bigipMgmtIPv4Address	12276 - 5	4	
bigipMgmtIPv6Address	12276 - 6	16	
contextName	12276 - 9	Variable	This IE is omitted for NetFlow v9.
contextType	12276 - 24	Variable	This IE is omitted for NetFlow v9.
observationTimeMilliseconds	323	8	
destinationGeo	12276 - 43	Variable	This IE is omitted for NetFlow v9.
destinationIPv4Address	12	4	
destinationIPv6Address	28	16	

Information Element (IE)	ID	Size (Bytes)	Notes
destinationTransportPort	11	2	
deviceProduct	12276 - 12	Variable	This IE is omitted for NetFlow v9.
deviceVendor	12276 - 11	Variable	This IE is omitted for NetFlow v9.
deviceVersion	12276 - 13	Variable	This IE is omitted for NetFlow v9.
dropReason	12276 - 40	Variable	This IE is omitted for NetFlow v9.
msgName	12276 - 14	Variable	This IE is omitted for NetFlow v9.
errdefsMsgNo	12276 - 4	4	
flowId	12276 - 3	8	
ipfixMsgNo	12276 - 16	4	
protocolIdentifier	4	1	
messageSeverity	12276 - 1	1	
partitionName	12276 - 2	Variable	This IE is omitted for NetFlow v9.
ingressVRFID	234	4	
saTransPool	12276 - 37	Variable	This IE is omitted for NetFlow v9.
saTransType	12276 - 36	Variable	This IE is omitted for NetFlow v9.
sourceGeo	12276 - 44	Variable	This IE is omitted for NetFlow v9.
sourceIPv4Address	8	4	
sourceIPv6Address	27	16	
sourceTransportPort	7	2	
sourceUser	12276 - 93	Variable	This IE is omitted for NetFlow v9.
transDestinationIPv4Address	12276 - 31	4	
transDestinationIPv6Address	12276 - 32	16	
transDestinationPort	12276 - 33	2	
transIpProtocol	12276 - 27	1	
transRouteDomain	12276 - 35	4	
transSourceIPv4Address	12276 - 28	4	
transSourceIPv6Address	12276 - 29	16	
transSourcePort	12276 - 30	2	
transVlanName	12276 - 34	Variable	This IE is omitted for NetFlow v9.
vlanName	12276 - 15	Variable	This IE is omitted for NetFlow v9.

DoS device

Information Element (IE)	ID	Size (Bytes)	Notes
action	12276 - 39	Variable	This IE is omitted for NetFlow v9.

Information Element (IE)	ID	Size (Bytes)	Notes
bigipHostName	12276 - 10	Variable	This IE is omitted for NetFlow v9.
bigipMgmtIPv4Address	12276 - 5	4	
bigipMgmtIPv6Address	12276 - 6	16	
contextName	12276 - 9	Variable	This IE is omitted for NetFlow v9.
observationTimeMilliseconds	323	8	
destinationIPv4Address	12	4	
destinationIPv6Address	28	16	
destinationTransportPort	11	2	
deviceProduct	12276 - 12	Variable	This IE is omitted for NetFlow v9.
deviceVendor	12276 - 11	Variable	This IE is omitted for NetFlow v9.
deviceVersion	12276 - 13	Variable	This IE is omitted for NetFlow v9.
dosAttackEvent	12276 - 41	Variable	This IE is omitted for NetFlow v9.
dosAttackId	12276 - 20	4	
dosAttackName	12276 - 21	Variable	This IE is omitted for NetFlow v9.
dosPacketsDropped	12276 - 23	4	
dosPacketsReceived	12276 - 22	4	
msgName	12276 - 14	Variable	This IE is omitted for NetFlow v9.
errdefsMsgNo	12276 - 4	4	
flowId	12276 - 3	8	
ipfixMsgNo	12276 - 16	4	
messageSeverity	12276 - 1	1	
partitionName	12276 - 2	Variable	This IE is omitted for NetFlow v9.
ingressVRFID	234	4	
sourceIPv4Address	8	4	
sourceIPv6Address	27	16	
sourceTransportPort	7	2	
vlanName	12276 - 15	Variable	This IE is omitted for NetFlow v9.

IP intelligence

Information Element (IE)	ID	Size (Bytes)	Notes
action	12276 - 39	Variable	This IE is omitted for NetFlow v9.
attackType	12276 - 46	Variable	This IE is omitted for NetFlow v9.
bigipHostName	12276 - 10	Variable	This IE is omitted for NetFlow v9.
bigipMgmtIPv4Address	12276 - 5	4	

Information Element (IE)	ID	Size (Bytes)	Notes
bigipMgmtIPv6Address	12276 - 6	16	
contextName	12276 - 9	Variable	This IE is omitted for NetFlow v9.
contextType	12276 - 24	Variable	This IE is omitted for NetFlow v9.
observationTimeMilliseconds	323	8	
destinationIPv4Address	12	4	
destinationIPv6Address	28	16	
destinationTransportPort	11	2	
deviceProduct	12276 - 12	Variable	This IE is omitted for NetFlow v9.
deviceVendor	12276 - 11	Variable	This IE is omitted for NetFlow v9.
deviceVersion	12276 - 13	Variable	This IE is omitted for NetFlow v9.
msgName	12276 - 14	Variable	This IE is omitted for NetFlow v9.
errdefsMsgNo	12276 - 4	4	
flowId	12276 - 3	8	
ipfixMsgNo	12276 - 16	4	
ipintelligencePolicyName	12276 - 45	Variable	This IE is omitted for NetFlow v9.
ipintelligenceThreatName	12276 - 42	Variable	This IE is omitted for NetFlow v9.
protocolIdentifier	4	1	
messageSeverity	12276 - 1	1	
partitionName	12276 - 2	Variable	This IE is omitted for NetFlow v9.
ingressVRFID	234	4	
saTransPool	12276 - 37	Variable	This IE is omitted for NetFlow v9.
saTransType	12276 - 36	Variable	This IE is omitted for NetFlow v9.
sourceIPv4Address	8	4	
sourceIPv6Address	27	16	
sourceTransportPort	7	2	
transDestinationIPv4Address	12276 - 31	4	
transDestinationIPv6Address	12276 - 32	16	
transDestinationPort	12276 - 33	2	
transIpProtocol	12276 - 27	1	
transRouteDomain	12276 - 35	4	
transSourceIPv4Address	12276 - 28	4	
transSourceIPv6Address	12276 - 29	16	
transSourcePort	12276 - 30	2	
transVlanName	12276 - 34	Variable	This IE is omitted for NetFlow v9.
vlanName	12276 - 15	Variable	This IE is omitted for NetFlow v9.

Log Throttle

Information Element (IE)	ID	Size (Bytes)	Notes
bigipHostName	12276 - 10	Variable	This IE is omitted for NetFlow v9.
bigipMgmtIPv4Address	12276 - 5	4	
bigipMgmtIPv6Address	12276 - 6	16	
observationTimeMilliseconds	323	8	
deviceProduct	12276 - 12	Variable	This IE is omitted for NetFlow v9.
deviceVendor	12276 - 11	Variable	This IE is omitted for NetFlow v9.
deviceVersion	12276 - 13	Variable	This IE is omitted for NetFlow v9.
msgName	12276 - 14	Variable	This IE is omitted for NetFlow v9.
errdefsMsgNo	12276 - 4	4	
ipfixMsgNo	12276 - 16	4	
messageSeverity	12276 - 1	1	
contextType	12276 - 24	Variable	This IE is omitted for NetFlow v9.
contextName	12276 - 9	Variable	This IE is omitted for NetFlow v9.
logprofileName	12276 - 95	Variable	This IE is omitted for NetFlow v9.
logMsgName	12276 - 97	Variable	This IE is omitted for NetFlow v9.
logMsgDrops	12276 - 96	4	

IPFIX Templates for AFM DNS Events

Overview: IPFIX Templates for AFM DNS Events

The IP Flow Information Export (IPFIX) Protocol is a logging mechanism for IP events. This appendix defines the IPFIX Information Elements (IEs) and Templates used to log F5's Application Firewall Manager (AFM) DNS events. An *IE* is the smallest form of useful information in an IPFIX log message, such as an IP address or a timestamp for the event. An *IPFIX template* is an ordered collection of specific IEs used to record one IP event, such as the denial of a DNS query.

About IPFIX Information Elements for AFM DNS events

Information Elements (IEs) are individual fields in an IPFIX template. An IPFIX template describes a single Advanced Firewall Manager™ (AFM™) DNS event.

IANA-defined IPFIX Information Elements

IANA maintains a list of standard IPFIX Information Elements (IEs), each with a unique Element Identifier. The F5® AFM™ DNS IPFIX implementation uses a subset of these IEs to publish AFM DNS events. This subset is summarized in the table.

Information Element (IE)	ID	Size (Bytes)
destinationIPv4Address	12	4
destinationIPv6Address	28	16
destinationTransportPort	11	2
ingressVRFID	234	4
observationTimeMilliseconds	323	8
sourceIPv4Address	8	4
sourceIPv6Address	27	16
sourceTransportPort	7	2

IPFIX enterprise Information Elements

IPFIX provides for enterprises to define their own Information Elements. F5® currently uses the following non-standard IEs for AFM™ DNS events:

Information Element (IE)	ID	Size (Bytes)
action	12276 - 39	Variable

Information Element (IE)	ID	Size (Bytes)
attackEvent	12276 - 41	Variable
attackId	12276 - 20	4
attackName	12276 - 21	Variable
bigipHostName	12276 - 10	Variable
bigipMgmtIPv4Address	12276 - 5	4
bigipMgmtIPv6Address	12276 - 6	16
contextName	12276 - 9	Variable
deviceProduct	12276 - 12	Variable
deviceVendor	12276 - 11	Variable
deviceVersion	12276 - 13	Variable
dnsQueryType	12276 - 8	Variable
errdefsMsgNo	12276 - 4	4
flowId	12276 - 3	8
ipfixMsgNo	12276 - 16	4
messageSeverity	12276 - 1	1
msgName	12276 - 14	Variable
packetsDropped	12276 - 23	4
packetsReceived	12276 - 22	4
partitionName	12276 - 2	Variable
queryName	12276 - 7	Variable
vlanName	12276 - 15	Variable

Note: *IPFIX, unlike NetFlow v9, supports variable-length IEs, where the length is encoded within the field in the Data Record. NetFlow v9 collectors (and their variants) cannot correctly process variable-length IEs, so they are omitted from logs sent to those collector types.*

About individual IPFIX Templates for each event

This section enumerates the IPFIX templates used by F5 to publish AFM DNS Events.

IPFIX template for DNS security

Information Element (IE)	ID	Size (Bytes)	Notes
action	12276 - 39	Variable	This IE is omitted for NetFlow v9.
bigipHostName	12276 - 10	Variable	This IE is omitted for NetFlow v9.

Information Element (IE)	ID	Size (Bytes)	Notes
bigipMgmtIPv4Address	12276 - 5	4	
bigipMgmtIPv6Address	12276 - 6	16	
contextName	12276 - 9	Variable	This IE is omitted for NetFlow v9.
observationTimeMilliseconds	323	8	
destinationIPv4Address	12	4	
destinationIPv6Address	28	16	
destinationTransportPort	11	2	
deviceProduct	12276 - 12	Variable	This IE is omitted for NetFlow v9.
deviceVendor	12276 - 11	Variable	This IE is omitted for NetFlow v9.
deviceVersion	12276 - 13	Variable	This IE is omitted for NetFlow v9.
queryName	12276 - 7	Variable	This IE is omitted for NetFlow v9.
dnsQueryType	12276 - 8	Variable	This IE is omitted for NetFlow v9.
errdefsMsgNo	12276 - 4	4	
flowId	12276 - 3	8	
ipfixMsgNo	12276 - 16	4	
messageSeverity	12276 - 1	1	
partitionName	12276 - 2	Variable	This IE is omitted for NetFlow v9.
ingressVRFID	234	4	
sourceIPv4Address	8	4	
sourceIPv6Address	27	16	
sourceTransportPort	7	2	
vlanName	12276 - 15	Variable	This IE is omitted for NetFlow v9.
msgName	12276 - 14	Variable	This IE is omitted for NetFlow v9.

IPFIX template for DNS DoS

Information Element (IE)	ID	Size (Bytes)	Notes
action	12276 - 39	Variable	This IE is omitted for NetFlow v9.
attackEvent	12276 - 41	Variable	This IE is omitted for NetFlow v9.
attackId	12276 - 20	4	
attackName	12276 - 21	Variable	This IE is omitted for NetFlow v9.
bigipHostName	12276 - 10	Variable	This IE is omitted for NetFlow v9.
bigipMgmtIPv4Address	12276 - 5	4	
bigipMgmtIPv6Address	12276 - 6	16	
contextName	12276 - 9	Variable	This IE is omitted for NetFlow v9.

Information Element (IE)	ID	Size (Bytes)	Notes
observationTimeMilliseconds	323	8	
destinationIPv4Address	12	4	
destinationIPv6Address	28	16	
destinationTransportPort	11	2	
deviceProduct	12276 - 12	Variable	This IE is omitted for NetFlow v9.
deviceVendor	12276 - 11	Variable	This IE is omitted for NetFlow v9.
deviceVersion	12276 - 13	Variable	This IE is omitted for NetFlow v9.
queryName	12276 - 7	Variable	This IE is omitted for NetFlow v9.
dnsQueryType	12276 - 8	Variable	This IE is omitted for NetFlow v9.
errdefsMsgNo	12276 - 4	4	
flowId	12276 - 3	8	
ipfixMsgNo	12276 - 16	4	
messageSeverity	12276 - 1	1	
partitionName	12276 - 2	Variable	This IE is omitted for NetFlow v9.
ingressVRFID	234	4	
sourceIPv4Address	8	4	
sourceIPv6Address	27	16	
sourceTransportPort	7	2	
vlanName	12276 - 15	Variable	This IE is omitted for NetFlow v9.
msgName	12276 - 14	Variable	This IE is omitted for NetFlow v9.
packetsDropped	12276 - 23	4	
packetsReceived	12276 - 22	4	

IPFIX Templates for AFM SIP Events

Overview: IPFIX Templates for AFM SIP Events

The IP Flow Information Export (IPFIX) Protocol is a logging mechanism for IP events. This appendix defines the IPFIX Information Elements (IEs) and Templates used to log F5's Application Firewall Manager (AFM) events related to the Session Initiation Protocol (SIP). An *IE* is the smallest form of useful information in an IPFIX log message, such as an IP address or a timestamp for the event. An *IPFIX template* is an ordered collection of specific IEs used to record one IP event, such as the acceptance of a SIP session.

About IPFIX Information Elements for AFM SIP events

Information Elements (IEs) are individual fields in an IPFIX template. An IPFIX template describes a single Advanced Firewall Manager™ (AFM™) SIP event.

IANA-defined IPFIX information elements

IANA maintains a list of standard IPFIX Information Elements (IEs), each with a unique Element Identifier. The F5® AFM™ SIP implementation uses a subset of these IEs to publish AFM SIP events. This subset is summarized in the table.

Information Element (IE)	ID	Size (Bytes)
destinationIPv4Address	12	4
destinationIPv6Address	28	16
destinationTransportPort	11	2
ingressVRFID	234	4
observationTimeMilliseconds	323	8
sourceIPv4Address	8	4
sourceIPv6Address	27	16
sourceTransportPort	7	2

IPFIX enterprise Information Elements

IPFIX provides for enterprises to define their own Information Elements. F5® currently uses the following non-standard IEs for AFM™ events:

Information Element (IE)	ID	Size (Bytes)
action	12276 - 39	Variable

Information Element (IE)	ID	Size (Bytes)
attackEvent	12276 - 41	Variable
attackId	12276 - 20	4
attackName	12276 - 21	Variable
bigipHostName	12276 - 10	Variable
bigipMgmtIPv4Address	12276 - 5	4
bigipMgmtIPv6Address	12276 - 6	16
contextName	12276 - 9	Variable
deviceProduct	12276 - 12	Variable
deviceVendor	12276 - 11	Variable
deviceVersion	12276 - 13	Variable
errdefsMsgNo	12276 - 4	4
flowId	12276 - 3	8
ipfixMsgNo	12276 - 16	4
messageSeverity	12276 - 1	1
msgName	12276 - 14	Variable
packetsDropped	12276 - 23	4
packetsReceived	12276 - 22	4
partitionName	12276 - 2	Variable
sipCallee	12276 - 19	Variable
sipCaller	12276 - 18	Variable
sipMethodName	12276 - 17	Variable
vlanName	12276 - 15	Variable

Note: *IPFIX, unlike NetFlow v9, supports variable-length IEs, where the length is encoded within the field in the Data Record. NetFlow v9 collectors (and their variants) cannot correctly process variable-length IEs, so they are omitted from logs sent to those collector types.*

About individual IPFIX Templates for each event

This section enumerates the IPFIX templates used by F5 to publish AFM SIP Events.

IPFIX template for SIP security

Information Element (IE)	ID	Size (Bytes)	Notes
action	12276 - 39	Variable	This IE is omitted for NetFlow v9.

Information Element (IE)	ID	Size (Bytes)	Notes
bigipHostName	12276 - 10	Variable	This IE is omitted for NetFlow v9.
bigipMgmtIPv4Address	12276 - 5	4	
bigipMgmtIPv6Address	12276 - 6	16	
contextName	12276 - 9	Variable	This IE is omitted for NetFlow v9.
observationTimeMilliseconds	323	8	
destinationIPv4Address	12	4	
destinationIPv6Address	28	16	
destinationTransportPort	11	2	
deviceProduct	12276 - 12	Variable	This IE is omitted for NetFlow v9.
deviceVendor	12276 - 11	Variable	This IE is omitted for NetFlow v9.
deviceVersion	12276 - 13	Variable	This IE is omitted for NetFlow v9.
errdefsMsgNo	12276 - 4	4	
flowId	12276 - 3	8	
ipfixMsgNo	12276 - 16	4	
messageSeverity	12276 - 1	1	
partitionName	12276 - 2	Variable	This IE is omitted for NetFlow v9.
ingressVRFID	234	4	
sipCallee	12276 - 19	Variable	This IE is omitted for NetFlow v9.
sipCaller	12276 - 18	Variable	This IE is omitted for NetFlow v9.
sipMethodName	12276 - 17	Variable	This IE is omitted for NetFlow v9.
sourceIPv4Address	8	4	
sourceIPv6Address	27	16	
sourceTransportPort	7	2	
vlanName	12276 - 15	Variable	This IE is omitted for NetFlow v9.
msgName	12276 - 14	Variable	This IE is omitted for NetFlow v9.

IPFIX template for SIP DoS

Information Element (IE)	ID	Size (Bytes)	Notes
action	12276 - 39	Variable	This IE is omitted for NetFlow v9.
attackEvent	12276 - 41	Variable	This IE is omitted for NetFlow v9.
attackId	12276 - 20	4	
attackName	12276 - 21	Variable	This IE is omitted for NetFlow v9.
bigipHostName	12276 - 10	Variable	This IE is omitted for NetFlow v9.
bigipMgmtIPv4Address	12276 - 5	4	

Information Element (IE)	ID	Size (Bytes)	Notes
bigipMgmtIPv6Address	12276 - 6	16	
contextName	12276 - 9	Variable	This IE is omitted for NetFlow v9.
observationTimeMilliseconds	323	8	
destinationIPv4Address	12	4	
destinationIPv6Address	28	16	
destinationTransportPort	11	2	
deviceProduct	12276 - 12	Variable	This IE is omitted for NetFlow v9.
deviceVendor	12276 - 11	Variable	This IE is omitted for NetFlow v9.
deviceVersion	12276 - 13	Variable	This IE is omitted for NetFlow v9.
errdefsMsgNo	12276 - 4	4	
flowId	12276 - 3	8	
ipfixMsgNo	12276 - 16	4	
messageSeverity	12276 - 1	1	
partitionName	12276 - 2	Variable	This IE is omitted for NetFlow v9.
ingressVRFID	234	4	
sipCallee	12276 - 19	Variable	This IE is omitted for NetFlow v9.
sipCaller	12276 - 18	Variable	This IE is omitted for NetFlow v9.
sipMethodName	12276 - 17	Variable	This IE is omitted for NetFlow v9.
sourceIPv4Address	8	4	
sourceIPv6Address	27	16	
sourceTransportPort	7	2	
vlanName	12276 - 15	Variable	This IE is omitted for NetFlow v9.
msgName	12276 - 14	Variable	This IE is omitted for NetFlow v9.
packetsDropped	12276 - 23	4	
packetsReceived	12276 - 22	4	

Index

A

access control, and SNMP data *112*
access levels, assigning *111–112*
active connections data, collecting using SNMP commands *108*
AFM
    IANA IPFIX IEs for *187*, *199*
    IPFIX template for DoS device events *190*
    IPFIX template for IP intelligence events *191*
    IPFIX template for log throttle events *193*
    IPFIX template for network session *189*
AFM DNS
    IANA IPFIX IEs for *195*
AFM-related SNMP traps, defined *116*
ASM-related SNMP traps, defined *117*
attack types
    and DNS DoS logs *169*
    and DNS logs *166*
    and DoS device protection *155*
authentication-related SNMP traps, defined *118*
AVR-related SNMP traps, defined *118*

B

BIG-IP system information *111*
BIG-IP system processes, monitoring using SNMP *100*

C

CGNAT high-speed logging, overview *67*
CGNAT IPFIX logging
    overview *73*
client access, allowing *111*
collectors
    for IPFIX *74*, *79*, *86*
connections
    collecting data about active *108*
    collecting data about HTTP *101*
    collecting data about new *107*
    collecting data about RAM *103*
    collecting data about SSL *104*
    collecting data about throughput *102*
control-plane logging, overview *33*
counters, sFlow *134*
CPU usage
    collecting based on a custom polling interval *106*
    collecting based on a predefined polling interval *105*
custom DNS profiles
    and disabling DNS logging *45*
    and enabling high-speed DNS logging *44*
    and logging DNS queries and responses *42–43*
    and logging DNS responses *43*
Customized IPFIX logging
    overview *85*
customized MIB entries
    about *109*
    creating *110*
custom log filters
    and disabling legacy system logging *37*
    and disabling logging *37*
    creating *36*
custom profiles
    and DoS Protection Logging *64*
    and Network Firewall Logging *56*, *81*
    and Protocol Security logging *50*

D

data sources
    viewing for sFlow *133*
default access levels, modifying *111*
destinations
    for IPFIX logging *75*, *80*, *87*
    for logging *35*, *41*, *49*, *55*, *63*, *69*
    for remote high-speed logging *35*, *41*, *49*, *55*, *63*, *69*
destination SNMP managers, specifying *114*
DNS DoS logs, and attack types *169*
DNS high-speed logging, overview *39*
DNS Logging
    disabling *45*
    enabling *44*
DNS Logging profile
    assigning to listener *44*
    assigning to virtual server *45*
DNS logging profiles, customizing *42–43*
DNS logs
    and attack types *166*
    and event IDs *165*
    and event messages *165*
DNS profiles
    and disabling DNS logging *45*
    and enabling high-speed DNS logging *44*
DoS device protection
    attack types *155*
DoS Protection logging
    customizing profiles *64*
    overview *61*
DoS-related SNMP traps, defined *119*
DS-Lite
    IPFIX template
        create inbound session *183*
        create outbound session *182*
        delete (finish) inbound session *184*
        delete (finish) outbound session *182*
        quota-exceeded event *185*
        translation failure *185*
dynamic routing, and viewing SNMP traps *100*

E

enterprise MIB files
    and SNMP *98*
    and viewing objects *100*
    downloading *99*

event examples
and BIG-IP system logs *170*
and Network DoS logs *161*
event IDs
and AFM logs *151*
and ASM logs *145*, *148*
and DNS DoS logs *168*
and DNS logs *165*
and Network DoS Protection logs *154*
and Protocol Security logs *163*
event messages
and AFM logs *151*
and ASM logs *145*, *148*
and DNS DoS logs *168*
and DNSlogs *165*
and Network DoS Protection logs *154*
and Protocol Security logs *163*
events
and AFM logs *152*, *163*, *167*, *170*
and ASM logs *146*, *150*
setting SNMP traps *113*

F

F5-BIGIP-COMMON-MIB.txt, and viewing SNMP traps *100*

G

general SNMP traps, defined *119*
GTM-related SNMP traps, defined *119*

H

hardware-related SNMP traps, defined *122*
high-availability system-related SNMP traps, defined *126*
high-speed logging
and CGNAT *67*
and DNS *39*
and server pools *34*, *40*, *48*, *54*, *62*, *68*
HOST-RESOURCES MIB, using in a script *100*
HTTP rates data, collecting using SNMP commands *101*
HTTP request logging
and code elements *30*
and profile settings *28*
HTTP request logging profile, overview *25*
HTTP samping data types, sFlow *137*

I

IPFIX
See also Creating custom elements
AFM DNS template overview *195*
AFM SIP template overview *199*
AFM template overview *187*
and server pools *74*, *79*, *86*
configuring a virtual server for customized logging with iRules *90*
standard elements *88*
statistics *91*
template
create inbound DS-Lite session *183*
IPFIX *(continued)*
template *(continued)*
create inbound NAT44 session *174*
create inbound NAT64 session *179*
create outbound DS-Lite session *182*
create outbound NAT44 session *173*
create outbound NAT64 session *177*
delete (finish) inbound DS-Lite session *184*
delete (finish) inbound NAT44 session *175*
delete (finish) inbound NAT64 session *179*
delete (finish) outbound DS-Lite session *182*
delete (finish) outbound NAT44 session *173*
delete (finish) outbound NAT64 session *178*
DS-Lite quota-exceeded event *185*
DS-Lite translation failure *185*
NAT44 PBA *177*
NAT44 quota-exceeded event *176*
NAT44 translation failure *176*
NAT64 PBA *181*, *186*
NAT64 quota-exceeded event *181*
NAT64 translation failure *180*
template for accept or deny through AFM firewall session *189*
template for AFM SIP security *200*
template for DNS DoS events *197*
template for DNS security events *196*
template for DoS device events *190*
template for IP intelligence events *191*
template for log throttle events *193*
template for SIP DoS *201*
template overview *171*
using an iRule to send custom IPFIX logs *88*, *94*
See also Creating custom elements
IPFIX collectors
and destinations for log messages *75*, *80*, *87*
and publishers for log messages *75*, *81*, *87*
IPFIX logging
and AFM *79*
and CGNAT, overview *73*
creating a destination *75*, *80*, *87*
with iRules, overview *85*
IPFIX logging, customized with iRules
result *95*
IPFIX logging, overview *79*

L

license-related SNMP traps, defined *127*
listeners
assigning DNS Logging profile *44*
log filters
and disabling system logging *37*
creating *36*
logging
and destinations *35*, *41*, *49*, *55*, *63*, *69*, *75*, *80*, *87*
and DoS Protection *61*
and DoS Protection profiles *64*
and network firewall *53*
and Network Firewall profiles *56*, *81*
and pools *34*, *40*, *48*, *54*, *62*, *68*, *74*, *79*, *86*
and Protocol Security *47*
and Protocol Security profiles *50*

logging *(continued)*
and publishers *36*, *42*, *50*, *56*, *64*, *70*, *75*, *81*, *87*
DNS queries and responses *42–43*
DNS responses *43*
system alerts *36*
logging profile
configuring LSN pools *71*, *76*
Logging profile
and network firewalls *58*, *65*
and Protocol Security events *51*
and the network firewall *82*
Logging profiles, disabling *52*, *58*, *65*
logging-related SNMP traps, defined *129*
log publisher
configuring LSN pools *71*, *76*
LSN
IANA IPFIX IEs for *171–172*
LSN logging profile
creating *70*, *76*
LSN pool
configuring *71*, *76*
LTM-related SNMP traps, defined *128*

M

memory usage data, collecting using SNMP commands *101*
MIB entries
about customizing *109*
customizing *110*
MIB files
about enterprise *98*
about RMON *109*
and viewing enterprise objects *100*

N

NAT44
IPFIX template
create inbound session *174*
create outbound session *173*
delete (finish) inbound session *175*
delete (finish) outbound session *173*
PBA *177*
quota-exceeded event *176*
translation failure *176*
NAT64
IPFIX template
create inbound session *179*
create outbound session *177*
delete (finish) inbound session *179*
delete (finish) outbound session *178*
PBA *181*, *186*
quota-exceeded event *181*
translation failure *180*
NET-SNMP MIB files, downloading *99*
Network DoS logs, and event examples *161*
Network DoS Protection logs
and event IDs *154*
and event messages *154*
Network Firewall logging
disabling *52*, *58*, *65*
Network Firewall Logging
customizing profiles *56*, *81*
network firewall logging, overview of high-speed remote *53*
Network Firewall Logging profile, assigning to virtual server *58*, *65*, *82*
network-related SNMP traps, defined *129*
new connections data, collecting using SNMP commands *107*
notifications, sending *114*

P

parameters
for HTTP request logging *30*
for request logging *30*
performance monitoring
and SNMP *97*
configuring on BIG-IP system *131*
permissions, and SNMP data objects *98*
polling interval
configuring global for sFlow *132*
configuring on an HTTP profile for sFlow *132*
configuring on interface for sFlow *133*
configuring on VLAN for sFlow *132*
pools
creating with request logging *25*
for high-speed logging *34*, *40*, *48*, *54*, *62*, *68*
for IPFIX *74*, *79*, *86*
prerequisites, and SNMP deployment *97*
profiles
and disabling DNS logging *45*
and disabling Network Firewall logging *52*, *58*, *65*
creating custom DNS logging *42*
creating custom DNS query and response logging *43*
creating custom DNS response logging *43*
creating for DNS logging *44*
creating for DoS Protection Logging *64*
creating for Network Firewall Logging *56*, *81*
creating for Protocol Security logging *50*
Protocol Security logging
customizing profiles *50*
overview *47*
Protocol Security Logging profile, assigning to virtual server *51*
publishers
and logging *75*, *81*, *87*
creating for logging *36*, *42*, *50*, *56*, *64*
publishers, and logging *70*

R

RAM cache data, collecting using SNMP commands *103*
receiver, adding sFlow to BIG-IP configuration *131*
remote servers
and destinations for log messages *35*, *41*, *49*, *55*, *63*, *69*
and publishers for log messages *70*
for high-speed logging *34*, *40*, *48*, *54*, *62*, *68*
request logging, and code elements *30*
request logging profile
creating *26*
deleting *28*
enabling for requests *26*
enabling for responses *27*
overview *25*

request logging profile *(continued)*
settings *28*
requests, accepting *111*
RMON MIB file, and SNMP *109*

S

sampling rate
configuring global for sFlow *132*
configuring on an HTTP profile for sFlow *132*
configuring on interface for sFlow *133*
configuring on VLAN for sFlow *132*
servers
and destinations for log messages *35*, *41*, *49*, *55*, *63*, *69*, *75*, *80*, *87*
and publishers for IPFIX logs *75*, *81*, *87*
and publishers for log messages *36*, *42*, *50*, *56*, *64*, *70*
for high-speed logging *34*, *40*, *48*, *54*, *62*, *68*
sFlow
configuring global polling interval and sampling rate *132*
configuring polling interval and sampling rate for an HTTP profile *132*
configuring polling interval and sampling rate for an interface *133*
configuring polling interval and sampling rate for a VLAN *132*
viewing data sources *133*
sFlow counters
defined *134*
sFlow HTTP sampling data types
defined *137*
sFlow receiver
adding to BIG-IP configuration *131*
configuring on BIG-IP system *131*
global settings *134*
settings *134*
sFlow VLAN sampling data types
defined *140*
SNMP
and deployment prerequisites *97*
and enterprise MIB files *98*
and monitoring BIG-IP system processes *100*
and the RMON MIB file *109*
configuring on BIG-IP system *97*
overview of components *98*
SNMP access levels, assigning *111*
SNMP agent configuration
overview of *111*
SNMP agents, allowing access to *111*
SNMP alerts, sending *113*
SNMP commands
collecting active connections data *108*
collecting HTTP rates data *101*
collecting memory usage data *101*
collecting new connections data *107*
collecting RAM cache data *103*
collecting SSL transactions *104*
collecting throughput rates data *102*
SNMP data
controlling access to *112*
SNMP data, and controlling access *112*
SNMP data objects, and permissions *98*
SNMP events, setting traps *113*
SNMP manager, and downloading MIB files *99*
SNMP notifications, sending *114*
SNMP protocol, managing *111*
SNMP traps
about troubleshooting *116*
and dynamic routing *100*
creating *115*
defined *113*
enabling *113*
table of advanced firewall manager-related *116*
table of application security management-related *117*
table of authentication-related *118*
table of AVR-related *118*
table of DoS-related *119*
table of general *119*
table of global traffic management-related *119*
table of hardware-related *122*
table of high-availability system-related *126*
table of license-related *127*
table of local traffic management-related *128*
table of logging-related *129*
table of network-related *129*
table of vCMP-related *130*
table of VIPRION-related *130*
viewing *100*, *115*
SNMP v1 and v2c traps, setting destination *114*
SNMP v3 traps, setting destination *114*
SSL transactions, collecting using SNMP commands *104*
status
viewing for sFlow data sources *133*
system information *111*
system log filters, customizing *36*
system logging
disabling *37*
disabling legacy *37*
overview *33*

T

TCL file, and customized MIB entries *110*
template, See IPFIX
throughput rates data, collecting using SNMP commands *102*
traps
about troubleshooting SNMP *116*
defined *113*
table of advanced firewall manager-related SNMP *116*
table of application security management-related SNMP *117*
table of authentication-related SNMP *118*
table of AVR-related SNMP *118*
table of DoS-related SNMP *119*
table of general SNMP *119*
table of global traffic management-related SNMP *119*
table of hardware-related SNMP *122*
table of high-availability system-related SNMP *126*
table of license-related SNMP *127*
table of local traffic management-related SNMP *128*
table of logging-related SNMP *129*
table of network-related SNMP *129*
table of vCMP-related SNMP *130*
table of VIPRION-related SNMP *130*

troubleshooting SNMP traps *116*
truncated log messages, and BIG-IP system logs *170*

V

vCMP-related SNMP traps, defined *130*
VIPRION-related SNMP traps, defined *130*
virtual server
  assigning Network Firewall Logging profile *58*, *65*, *82*
  assigning Protocol Security Logging profile *51*
  configuring for IPFIX logging with iRules *90*
virtual servers
  assigning a Request Logging profile *27*
  assigning DNS Logging profile *45*
  creating an iRule for customized IPFIX logs *88*, *94*
VLAN samping data types, sFlow *140*