BIG-IP® DNS Services: Implementations

Version 11.5

Table of Contents

Legal Notices

Publication Date

This document was published on January 27, 2014.

Publication Number

MAN-0446-02

Copyright

Trademarks

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.

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.

Chapter 1

Configuring DNS Express

What is DNS Express?

DNS Express™ is an engine that provides the ability for the BIG-IP® system to act as a high-speed, authoritative DNS server. With DNS Express configured, the BIG-IP system can answer DNS queries for a DNS zone and respond to zone transfer requests from specified DNS nameservers (clients). Additionally, zone transfer communications can be secured with TSIG keys.

About configuring DNS Express

You can configure the BIG-IP system to use the DNS Express™ engine to answer queries for a DNS zone. This involves a zone transfer from the authoritative DNS server into DNS Expres,s and then DNS Express can answer DNS queries for the zone. For this configuration you create the following objects in the order described.

TSIG key (optional)
Obtain the TSIG key data from the authoritative DNS server that hosts the zone and create a TSIG key object.

Nameserver object
Create a nameserver object to represent the authoritative DNS server. Optionally, add the TSIG key.

DNS zone
Create a zone object and in the DNS Express area, select the nameserver object that represents the authoritative DNS server that hosts the zone.

Custom DNS profile (optional)
Create a custom DNS profile based on your network architecture.

DNS listener or LTM virtual server
Create a DNS listener or LTM virtual server and select a DNS profile. You can use either the default DNS profile or the custom DNS profile.

Additionally, you can configure the BIG-IP system to use the DNS Express™ engine to answer zone transfer requests for a DNS zone from a DNS nameserver that answers DNS queries. For this configuration you create or modify the following objects in the order described.

TSIG key (optional)
Obtain the TSIG key data from the DNS nameserver client that you want to allow to send zone transfer requests for the DNS zone and create a TSIG key object.

Nameserver object
Create a nameserver object to represent the DNS nameserver that will make the zone transfer request. Optionally, add the TSIG key.

DNS zone
Modify the zone object to add zone transfer clients to the zone. In the Zone Transfer Clients area, select the nameserver object you created.

Custom DNS profile (optional)
Modify the DNS profile to allow zone transfers from the BIG-IP system to the client.

Configuring DNS Express to answer DNS queries

DNS Express can answer DNS queries for a DNS zone configured on and transferred to the BIG-IP system. Optionally, DNS Express can use TSIG keys to validate zone transfer communications between the BIG-IP system and the authoritative DNS server hosting the zone.

Example of loading a zone into DNS Express

In this figure, an administrator at Site Request creates a DNS zone with a DNS Express™ server. The name of the DNS zone on the BIG-IP® system matches the name of the zone on the authoritative DNS server. The creation of the zone initiates a zone transfer request from DNS Express to the authoritative DNS server that hosts the zone. The server responds with a zone transfer and the zone is loaded into the DNS Express engine.

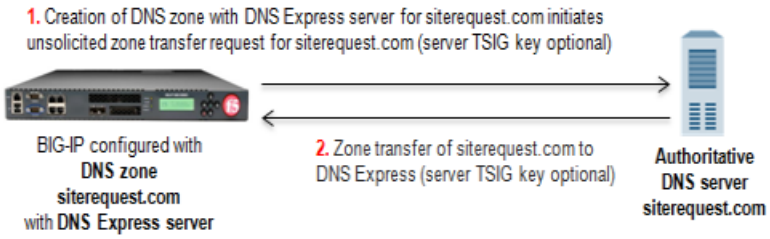


Figure 1: DNS zone transfer to DNS Express

1. Creation of siterequest.com DNS zone with a DNS Express server on the BIG-IP system initiates an unsolicited zone transfer request.
2. Authoritative DNS server responds with zone transfer and DNS Express loads the zone.

Example of DNS Express answering DNS queries

In this figure, as the zone is updated, the authoritative DNS server sends a NOTIFY to DNS Express, which responds with a zone transfer request. The server responds with a zone transfer and the zone is updated in DNS Express. When the LDNS sends a query for the zone, DNS Express can answer the query faster than the authoritative DNS server.

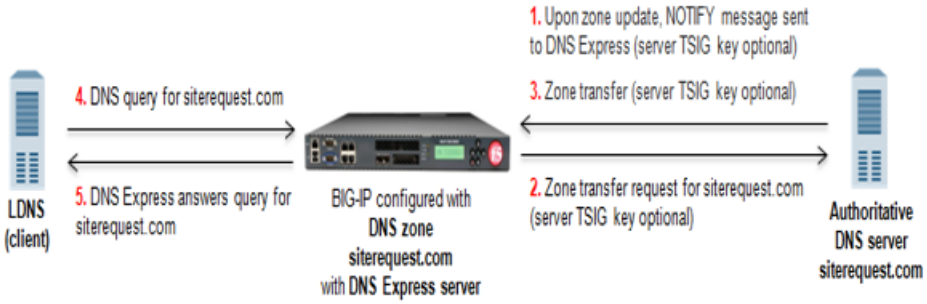


Figure 2: DNS Express answering queries for a DNS zone

1. When zone update occurs, DNS server sends NOTIFY message to DNS Express.
2. DNS Express sends zone transfer request in response.
3. DNS server answers with zone transfer and DNS Express updates the zone.
4. LDNS sends DNS query for the zone.
5. DNS Express answers with authoritative response. The response is faster than the authoritative DNS server.

About TSIG key authentication

The BIG-IP® system can use transaction signature (TSIG) keys to authenticate communications about zone transfers between the BIG-IP system and authoritative DNS servers, and between the BIG-IP system and DNS nameservers (clients). TSIG keys are generated by a third party tool such as BIND's keygen utility. Using TSIG keys is optional.

TSIG key configured on authoritative DNS server

You can add a TSIG key to a nameserver object that represents an authoritative DNS server. With this configuration, when the DNS server sends a NOTIFY message to the BIG-IP system, DNS Express™ responds with a TSIG-signed zone transfer request. Then the DNS server returns a TSIG-signed zone transfer. If required, you can disable the **Verify Notify TSIG** option on the DNS zone. With this configuration, DNS Express can process a NOTIFY message without a TSIG key, even when a subsequent zone transfer requires a TSIG key.

TSIG key configured on DNS nameserver (client)

You can add a TSIG key to a nameserver object that represents a DNS nameserver (client). When the client sends a TSIG-signed zone transfer request, DNS Express returns a TSIG-signed zone transfer.

TSIG key configured on DNS zone

You can add a server TSIG key to a DNS zone on the BIG-IP system. With this configuration, the system uses this TSIG key when the zone on the BIG-IP system is a proxy for the zone on the server. There are two possible scenarios:

- Client sends TSIG-signed zone transfer request

  When the BIG-IP system receives a TSIG-signed zone transfer request from a client for a DNS zone for which it is a proxy, the system validates the client TSIG key and removes the key from the request. The system then adds the server TSIG key to the request and forwards the TSIG-signed request to the DNS server or load balances the TSIG-signed request to a pool of DNS servers. The DNS server responds with a TSIG-signed zone transfer. The BIG-IP system validates the server TSIG key and removes the key. Then the system adds the client TSIG key and returns a TSIG-signed signed zone transfer to the client.

- Client sends unsigned zone transfer request

  When the BIG-IP system receives an unsigned zone transfer request from a client for a DNS zone for which it is a proxy, the system adds the server TSIG key to the request. The system then forwards the TSIG-signed request to the DNS server or load balances the TSIG-signed request to a pool of DNS servers. The DNS server responds with a TSIG-signed zone transfer. The BIG-IP system validates the server TSIG key and removes the key. Then the system returns an unsigned zone transfer to the client.

About listeners

A *listener* is a specialized virtual server that passively checks for DNS packets on port 53 and the IP address you assign to the listener. When a DNS request is sent to the IP address of the listener, the BIG-IP® system either handles the request or forwards the request to the appropriate resource.

Task summary

Perform these tasks to configure DNS Express™ to answer DNS queries for a DNS zone:

Configuring BIND servers to allow zone transfers
Configuring local BIND to send NOTIFY messages to DNS Express
Adding TSIG keys
Adding namserver objects that represent DNS servers
Creating a DNS zone to answer DNS queries
Disabling TSIG verification for NOTIFY messages
Optional: Enabling DNS Express with a custom DNS profile
Creating listeners to identify DNS Express traffic
Creating virtual servers to identify DNS Express traffic
Viewing DNS zone statistics

Configuring BIND servers to allow zone transfers

If you are unfamiliar with how to modify DNS server files, review the fifth edition of *DNS and BIND*, available from O'Reilly Media.

Typically, BIND servers allow zone transfers to any DNS nameserver requesting a zone transfer. That is, `named.conf` on a typical BIND server does not contain an allow-transfer statement. However, the BIND server on the BIG-IP® system is configured to allow zone transfers to only the localhost. Thus, `named.conf` on the BIG-IP system contains this allow-transfer statement: `allow-transfer { localhost; } ;`.

When you want to improve the speed of responses to DNS queries you can configure a BIND server to allow zone transfers only to the DNS Express™ engine on the BIG-IP system. You do this by adding an allow-transfer statement to `named.conf` on the BIND server.

Note: *Adding an allow-transfer statement to a BIND server actually restricts zone transfers to a specified list of DNS nameservers.*

Add to the BIND server an allow-transfer statement that specifies a self IP address on the BIG-IP system.

You can modify the following allow-transfer statement to use a self IP address on the BIG-IP system:

```
allow-transfer {
        localhost; <self IP address from which zone transfer request is sent
 to the server>;
    };
```

```
allow-transfer { localhost; 10.10.10.1 ; };
```

Configuring local BIND to send NOTIFY messages to DNS Express

When you configure an allow-transfer statement in `named.conf` on the local BIND server on the BIG-IP system to allow zone transfers only to DNS Express, you must include an `also-notify` statement that directs NOTIFY messages from local BIND to DNS Express.

Add to `named.conf` on the local BIND, an `also-notify` statement that specifies the BIG-IP system use this loopback address and port: `::1 port 5353` globally.

Note: *If you prefer, you can configure the `also-notify` statement on a per-zone or per view basis.*

```
also-notify {
                ::1 port 5353;
             };
```

Adding TSIG keys

- If you are adding TSIG keys for DNS servers that host zones:
  - Ensure that the DNS servers are configured to allow the BIG-IP system to perform zone transfers.
  - Ensure that the time on the systems that use TSIG keys are sychronized.
  - Obtain the TSIG key for each DNS server.
- If you are adding TSIG keys for DNS nameservers (clients)
  - Ensure that the time on the systems that use TSIG keys are sychronized.
  - Obtain the TSIG key for each client.

Note: *TSIG keys are created by a third party tool such as BIND's keygen utility.*

Add TSIG keys to the BIG-IP system configuration, in these cases:

- When you want to validate zone transfer communications between DNS Express and a DNS server.
- When you want to validate zone transfer communications between DNS Express and a DNS nameserver (client).

1. On the Main tab, click **DNS** > **Delivery** > **Keys** > **TSIG Key List**.
   The TSIG Key List screen opens.
2. Click **Create**.
   The New TSIG Key screen opens.
3. In the **Name** field, type the name of the TSIG key.
4. From the Algorithm list, select the algorithm that was used to generate the key.
5. In the **Secret** field, type the TSIG key secret.
6. Click **Finished**.
7. Create additional TSIG keys on the BIG-IP system for each DNS server and each client that require authentication of communications.

Add the TSIG keys to DNS nameservers and DNS zones on the BIG-IP system.

Adding namserver objects that represent DNS servers

Obtain the IP address of the authoritative DNS server that hosts the DNS zone. Optional: Ensure that the server TSIG key is available on the BIG-IP system.

When you want to transfer a zone from an authoritative DNS server into the DNS Express™ engine and have DNS Express respond to DNS queries for the zone, add a nameserver object that represents the server that hosts the zone.

1. On the Main tab, click **DNS** > **Delivery** > **Nameservers**.
   The Nameservers List screen opens.
2. Click **Create**.
   The New Nameserver screen opens.
3. In the **Name** field, type a name for the authoritative DNS server.
4. In the **Address** field, type the IP address on which the DNS server listens for DNS messages.
5. Optional: From the **Server Key** list, select the TSIG key that matches the TSIG key on the DNS server.
   The BIG-IP system uses this TSIG key to sign DNS zone transfer requests sent to the DNS server that hosts this zone, and then to verify a zone transfer returned from the DNS server.

Create a DNS zone and add a DNS Express server object to the zone.

Creating a DNS zone to answer DNS queries

Do the following before you create a DNS zone:

- Ensure that the authoritative DNS server that currently hosts the zone is configured to allow zone transfers to the BIG-IP system.
- Ensure a nameserver object that represents the authoritative DNS server exists in the BIG-IP system configuration.
- Determine the name you want to use for the zone. The zone name must match the zone name on the authoritative DNS server exactly.

Note: *Zone names are case insensitive.*

Create a DNS zone on the BIG-IP® system when you want the DNS Express engine to answer DNS queries for the zone.

1. On the Main tab, click **DNS** > **Zones**.
   The Zone List screen opens.
2. Click **Create**.
   The New Zone screen opens.
3. In the **Name** field, type the name of the DNS zone.
   The name must begin and end with a letter and contain only letters, numbers, and the period and hyphen (-) characters.
4. In the DNS Express area, from the **Server** list, select the authoritative primary DNS server that currently hosts the zone.

Note: *The DNS Express engine requests zone transfers from this server.*

---

5. From the **Notify Action** list, select one of the following to specify the action the BIG-IP system takes after receiving a NOTIFY message for this zone.

Action	Description
Consume	The BIG-IP system processes the NOTIFY message and does not pass the NOTIFY message to the back end DNS server.
Bypass	The BIG-IP system does not process the NOTIFY message, but instead sends the NOTIFY message to the back end DNS server (subject to DNS profile unhandled-query-action).
Repeat	The BIG-IP system processes the NOTIFY message and sends the NOTIFY message to the back end DNS server.

Tip: *If the nameserver object for the DNS server is configured with a TSIG Key, the signature is only validated for* ***Consume*** *and* ***Repeat*** *actions. Additionally, NOTIFY responses are assumed to be sent by the DNS server, except when the action is* ***Consume*** *and the DNS Express engine generates the response.*

6. Click **Finished**.

Disabling TSIG verification for NOTIFY messages

The BIG-IP® system might need to accept a zone transfer for a DNS Express™ zone from an authoritative DNS server, even if the NOTIFY message does not contain a TSIG key. To configure the system for this scenario, you can disable TSIG verification for NOTIFY messages, as an option.

1. On the Main tab, click **DNS** > **Zones**.
   The Zone List screen opens.
2. Click the name of the zone you want to modify.
3. From the **DNS Express** list, select **Advanced**.
4. Clear the **Verify Notify TSIG** check box.
5. Click **Update**.

Optional: Enabling DNS Express with a custom DNS profile

The BIG-IP® system contains a default DNS profile on which DNS Express™ is enabled. However, you can create a custom DNS profile to work with your network architecture.

Note: *If you plan to use the BIND server on a BIG-IP GTM™ system, use the default* ***dns*** *profile.*

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. Name the profile `dns_express`.
4. In the **Parent Profile** list, accept the default **dns** profile.
5. Select the **Custom** check box.
6. From the **Global Traffic Management** list, select **Disabled**.

7. From the **DNS Express** list, retain the default value **Enabled**.
8. From the **Unhandled Query Actions** list, select how you want the BIG-IP system to handle a query that is not for a wide IP or DNS Express zone.

Option	Description
Allow	The BIG-IP system forwards the query to a DNS server or a member of a pool of DNS servers. Note that if the pool is not associated with a listener and the **Use BIND Server on BIG-IP** option is set to **enabled**, queries are forwarded to the local BIND server. (Allow is the default value.)
Drop	The BIG-IP system does not respond to the query.
Reject	The BIG-IP system returns the query with the REFUSED return code.
Hint	The BIG-IP system returns the query with a list of root name servers.
No Error	The BIG-IP system returns the query with the NOERROR return code.

9. From the **Use BIND Server on BIG-IP** list, select **Disabled**.
10. Click **Finished**.

Assign the profile to virtual servers or listeners.

Creating listeners to identify DNS Express traffic

Create listeners to identify the DNS queries that DNS Express handles. When DNS Express™ is only answering DNS queries, only two listeners are required: one with an IPv4 address that handles UDP traffic and one with an IPv6 address that handles UDP traffic.

However, the best practice is to create four listeners, which allows DNS Express to handle zone transfers, should you decide to use this feature. DNS zone transfers use TCP port `53`. With this configuration, you create one listener with an IPv4 address that handles UDP traffic, and one with the same IPv4 address that handles TCP traffic. You also create one listener with an IPv6 address that handles UDP traffic, and one with the same IPv6 address that handles TCP traffic.

Tip: *If you have multiple BIG-IP® GTM™ systems in a device group, perform these steps on only one system.*

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 **Create**.
   The Listeners properties screen opens.
3. In the **Name** field, type a unique name for the listener.
4. For the Destination setting, in the **Address** field, type an IPv4 address on which the BIG-IP system listens for DNS queries.
5. From the **Listener** list, select **Advanced**.
6. Optional: If you are using SNATs on your network, from the **Source Address Translation** list, select **SNAT**.
7. Optional: If you are using NATs on your network, for the **Address Translation** setting, select the **Enabled** check box.
8. Optional: If you are using port translation on your network, for the **Port Translation** setting, select the **Enabled** check box.

9. In the Service area, from the **Protocol** list, select **UDP**.
10. In the Service area, from the **DNS Profile** list, select either **dns** or a custom DNS profile configured for DNS Express.
11. Click **Finished**.

Create another listener with the same IPv4 address and configuration, but select **TCP** from the **Protocol** list. Then, create two more listeners, configuring both with the same IPv6 address, but one with the UDP protocol and one with the TCP protocol.

Creating virtual servers to identify DNS Express traffic

Create virtual servers to process the DNS queries that DNS Express handles. When DNS Express is only answering DNS queries, only two virtual servers are required: one with an IPv4 address that handles UDP traffic and one with an IPv6 address that handles UDP traffic.

However, the best practice is to create four listeners, which allows DNS Express to handle zone transfers, should you decide to use this feature. DNS zone transfers use TCP port `53`. With this configuration, you create one virtual server with an IPv4 address that handles UDP traffic, and one with the same IPv4 address that handles TCP traffic. You also create one virtual server with an IPv6 address that handles UDP traffic, and one with the same IPv6 address that handles TCP traffic.

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 **Create** button.
   The New Virtual Server screen opens.
3. In the **Name** field, type a unique name for the virtual server.
4. For the **Destination** setting, in the **Address** field, type the IP address you want to use for the virtual server.
5. In the **Service Port** field, type **53**.
6. From the **Protocol** list, select **UDP**.
7. Optional: If you are using SNATs on your network, from the **Source Address Translation** list, select **SNAT**.
8. Optional: From the **SNAT pool** list, select the name of an existing SNAT pool.
9. From the **Configuration** list, select **Advanced**.
10. From the **DNS Profile** list, select either **dns** or the custom DNS profile you created for DNS Express.
11. Click **Finished**.

Create another virtual server with the same IPv4 address and configuration, but select **TCP** from the **Protocol** list. Then, create two more virtual servers, configuring both with the same IPv6 address, but one with the UDP protocol and one with the TCP protocol.

Task summary

Viewing DNS zone statistics

You can view information about DNS zones.

1. On the Main tab, click **Statistics** > **Module Statistics** > **DNS** > **Zones**.

The Zones statistics screen opens.

2. From the **Statistics Type** list, select **Zones**.
   Information displays about the traffic handled by the zones in the list.
3. In the Details column for a zone, click **View**.
   Read the online help for an explanation of the statistics.

Configuring DNS Express to answer zone transfer requests

DNS Express™ can respond to zone transfer requests for a DNS zone from specified DNS nameservers (clients). Optionally, DNS Express can use TSIG keys to validate the identity of the client making the zone transfer request.

Example of DNS Express answering zone transfer requests

In this figure, as the zone is updated, the authoritative DNS server sends a NOTIFY to DNS Express, which responds with a zone transfer request. The server responds with a zone transfer and the zone is updated in DNS Express. DNS Express sends a NOTIFY to the client, and the client responds with a zone transfer request for the zone. DNS Express responds with a zone transfer and the client updates the zone.

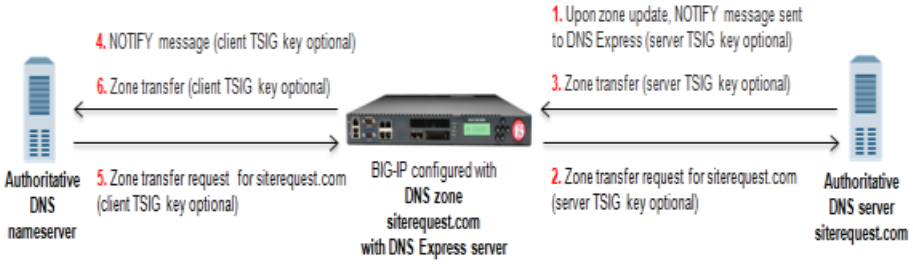


Figure 3: DNS Express answering zone transfer requests for DNS zone

1. When zone update occurs, the DNS server sends NOTIFY message to DNS Express.
2. DNS Express sends zone transfer request as a result of the NOTIFY query.
3. DNS server answers with zone transfer and DNS Express updates the zone.
4. DNS Express sends NOTIFY to authoritative DNS nameserver client.
5. Client sends zone transfer request as a result of the NOTIFY query.
6. DNS Express answers with zone transfer of siterequest.com, and client updates the zone.

Task summary

To configure the BIG-IP® system to respond to zone transfer requests, perform these tasks:

Adding nameserver objects that represent DNS nameservers (clients)
Configuring DNS Express to answer zone transfer requests from specified clients
Enabling DNS Express to respond to a zone transfer request

Adding nameserver objects that represent DNS nameservers (clients)

Gather the IP addresses of the DNS nameservers (clients) from which the DNS Express™ engine accepts zone transfer requests for a DNS zone. Optional: Ensure that the client TSIG key is available on the BIG-IP system.

To allow DNS nameservers (clients) to request zone transfers for a zone, add a nameserver object that represents each client. Optionally, you can add a client TSIG key that the BIG-IP system uses to authenticate the identity of the client during zone transfer communications.

1. On the Main tab, click **DNS** > **Delivery** > **Nameservers**.
   The Nameservers List screen opens.
2. Click **Create**.
   The New Nameserver screen opens.
3. In the **Name** field, type a name for the DNS nameserver (client).
4. In the **Address** field, type the IP address on which the DNS nameserver (client) listens for DNS messages.
5. Optional: If you want the BIG-IP system to validate a zone transfer request from this client, from the **TSIG Key** list, select the client TSIG key.

   If there is a TSIG key configured on this client, the BIG-IP system uses the key to validate a zone transfer request from this client, and adds a signature for this key to a zone transfer response sent from a DNS server, a pool member, or DNS Express.
6. Click **Finished**.
7. Add nameserver objects to represent other DNS nameservers (clients).

Add the DNS nameservers (clients) objects to the **Zone Transfer Client** list of the DNS zone on the BIG-IP system.

Configuring DNS Express to answer zone transfer requests from specified clients

Ensure that nameserver objects exist in the BIG-IP® system configuration that represent the DNS server that hosts the zone and the DNS nameservers (clients) that are permitted to request zone transfers.

You can configure DNS Express™ to respond to zone transfer requests for a specific zone by adding nameservers to the **Zone Transfer Clients** list for the zone.

1. On the Main tab, click **DNS** > **Zones**.
   The Zone List screen opens.
2. Click the name of the zone you want to modify.
3. In the Zone Transfer Clients area, move the nameservers that can initiate zone transfers from the **Available** list to the **Active** list.
4. Click **Finished**.

The nameservers in the **Active** list can initiate zone transfer requests for this zone.

Enabling DNS Express to respond to a zone transfer request

DNS zone transfers use TCP port `53`. Ensure that a listener configured for TCP exists in the configuration.

To enable DNS Express to answer zone transfers for a zone, modify the DNS profile assigned to the listener.

1. On the Main tab, click **DNS** > **Delivery** > **Profiles** > **DNS** or **Local Traffic** > **Profiles** > **Services** > **DNS**.
   The DNS profile list screen opens.
2. In the Name column, click the name of the profile you want to modify.
3. Select the **Custom** check box.
4. From the **Zone Transfer** list, select **Enabled**.
5. Click **Finished**.

Chapter 2

Configuring a DNS Zone Proxy

Overview: Configuring a DNS zone proxy

Within your network, the BIG-IP® system can act as a proxy for an authoritative DNS server. In this case, when the BIG-IP system receives a zone transfer request from a specified list of DNS namservers (clients), the system sends the request to the authoritative DNS server. The server responds with a zone transfer, and the BIG-IP system sends the zone transfer to the client that made the zone transfer request. Optionally, the BIG-IP system can use transaction signature (TSIG) keys to validate the identity of the authoritative DNS server sending a zone transfer and the DNS nameservers (clients) sending zone transfer requests.

Example of DNS zone proxy with client-side TSIG authentication

In this figure, an administrator at Site Request creates a DNS zone on the BIG-IP system that is a proxy for the zone on the authoritative DNS server that hosts the zone. The name of the DNS zone on the BIG-IP system matches the name of the zone on the authoritative DNS server. The administrator uses TSIG key authenthication to verify the zone transfer communications between the BIG-IP system and the DNS nameserver (client) making the zone transfer request.

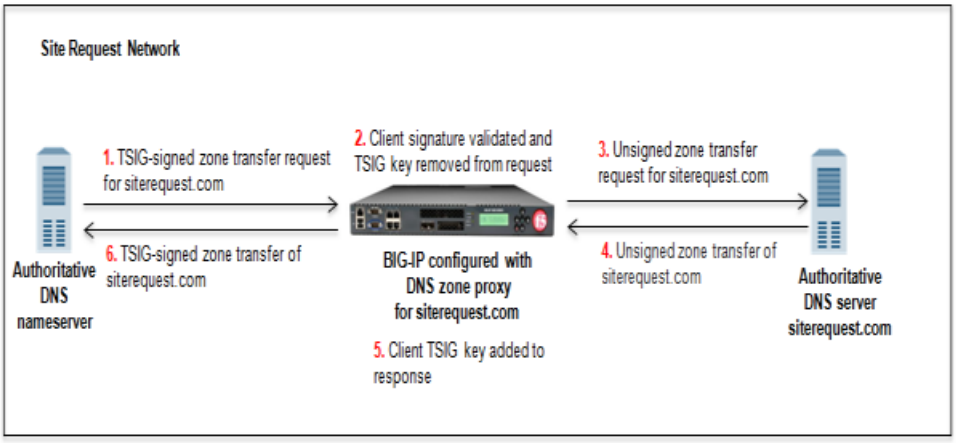


Figure 4: BIG-IP system acting as DNS zone proxy with client-side TSIG authentication

1. DNS nameserver (client) sends TSIG-signed zone transfer request for a DNS zone.
2. BIG-IP system validates the signature and removes the client TSIG key.
3. BIG-IP system sends the unsigned request to the DNS server that hosts the zone.
4. DNS server answers with an unsigned zone transfer to the BIG-IP system.
5. BIG-IP system adds the client TSIG key to the response.
6. BIG-IP system sends a TSIG-signed zone transfer to the DNS nameserver that made the request.

Example of DNS zone proxy with client-side and server-side TSIG authentication

In this figure, an administrator at Site Request creates a DNS zone on the BIG-IP system that is a proxy for the zone on the authoritative DNS server that hosts the zone. The name of the DNS zone on the BIG-IP system matches the name of the zone on the authoritative DNS server. The administrator uses TSIG key authenthication to verify the zone transfer communications between the BIG-IP system and the authoritative DNS server and between the BIG-IP system and the client making a zone transfer request.

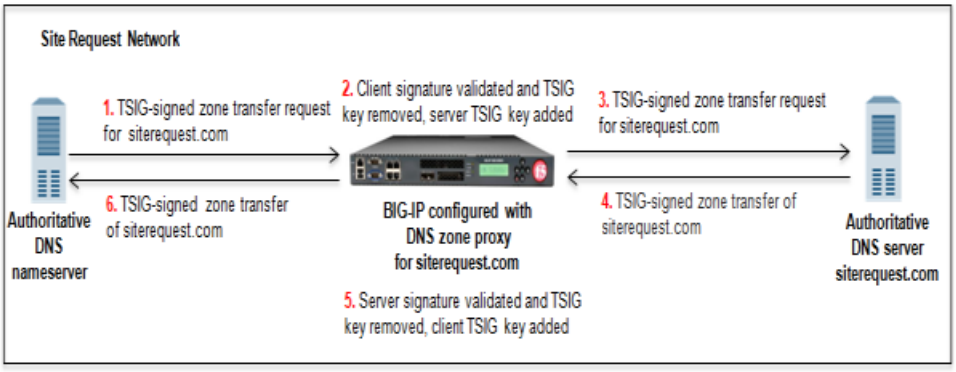


Figure 5: BIG-IP system acting as DNS zone proxy with client and server-side TSIG authentication

1. DNS nameserver (client) sends TSIG-signed zone transfer request for a DNS zone.
2. BIG-IP system validates the signature, removes the client TSIG key from the request, and adds the server TSIG key to the request.
3. BIG-IP system sends the TSIG-signed request to the DNS server that hosts the zone.
4. DNS server answers with a TSIG-signed zone transfer to the BIG-IP system.
5. BIG-IP system validates the signature, removes the server TSIG key from the response, and adds the client TSIG key to the response.
6. BIG-IP system sends the TSIG-signed zone transfer to the DNS nameserver that made the request.

About TSIG key authentication

The BIG-IP® system can use transaction signature (TSIG) keys to authenticate communications about zone transfers between the BIG-IP system and authoritative DNS servers, and between the BIG-IP system and DNS nameservers (clients). TSIG keys are generated by a third party tool such as BIND's keygen utility. Using TSIG keys is optional.

TSIG key configured on authoritative DNS server

You can add a TSIG key to a nameserver object that represents an authoritative DNS server. With this configuration, when the DNS server sends a NOTIFY message to the BIG-IP system, DNS Express™ responds with a TSIG-signed zone transfer request. Then the DNS server returns a TSIG-signed zone transfer. If required, you can disable the **Verify Notify TSIG** option on the DNS zone. With this configuration, DNS Express can process a NOTIFY message without a TSIG key, even when a subsequent zone transfer requires a TSIG key.

TSIG key configured on DNS nameserver (client)

You can add a TSIG key to a nameserver object that represents a DNS nameserver (client). When the client sends a TSIG-signed zone transfer request, DNS Express returns a TSIG-signed zone transfer.

TSIG key configured on DNS zone

You can add a server TSIG key to a DNS zone on the BIG-IP system. With this configuration, the system uses this TSIG key when the zone on the BIG-IP system is a proxy for the zone on the server. There are two possible scenarios:

- Client sends TSIG-signed zone transfer request

  When the BIG-IP system receives a TSIG-signed zone transfer request from a client for a DNS zone for which it is a proxy, the system validates the client TSIG key and removes the key from the request. The system then adds the server TSIG key to the request and forwards the TSIG-signed request to the DNS server or load balances the TSIG-signed request to a pool of DNS servers. The

DNS server responds with a TSIG-signed zone transfer. The BIG-IP system validates the server TSIG key and removes the key. Then the system adds the client TSIG key and returns a TSIG-signed signed zone transfer to the client.

- Client sends unsigned zone transfer request

  When the BIG-IP system receives an unsigned zone transfer request from a client for a DNS zone for which it is a proxy, the system adds the server TSIG key to the request. The system then forwards the TSIG-signed request to the DNS server or load balances the TSIG-signed request to a pool of DNS servers. The DNS server responds with a TSIG-signed zone transfer. The BIG-IP system validates the server TSIG key and removes the key. Then the system returns an unsigned zone transfer to the client.

About listeners

A *listener* is a specialized virtual server that passively checks for DNS packets on port 53 and the IP address you assign to the listener. When a DNS request is sent to the IP address of the listener, the BIG-IP® system either handles the request or forwards the request to the appropriate resource.

Task summary

Perform these tasks to configure a DNS zone on the BIG-IP system that is a proxy for a DNS zone on a DNS server in your network:

Configuring BIND servers to allow zone transfers
Adding TSIG keys for DNS zone proxy
Adding DNS nameserver (client) objects
Enabling zone transfers
Creating a DNS zone
Creating listeners to forward zone transfer requests
Creating virtual servers to forward zone transfer requests

Configuring BIND servers to allow zone transfers

If you are unfamiliar with how to modify BIND server files, review the fifth edition of *DNS and BIND*, available from O'Reilly Media.

Typically, BIND servers allow zone transfers to any DNS nameserver requesting a zone transfer. That is, `named.conf` on a typical BIND server does not contain an allow-transfer statement. Therefore, adding an allow-transfer statement to a BIND server actually restricts zone transfers to a specified list of DNS nameservers.

When you want the BIG-IP® system to act as a proxy for a DNS zone configured on a BIND server, you must add an *allow-transfer* statement to `named.conf` on the BIND server that hosts the zone.

Here is an example allow-transfer statement that you can modify to meet your needs: `allow-transfer { localhost; <self IP address on BIG-IP from which zone transfer request is sent to the DNS server>; };`

```
allow-transfer { localhost; 10.10.10.1 ; };
```

Adding TSIG keys for DNS zone proxy

Obtain the TSIG keys that you want to add to the BIG-IP® system for the DNS server that hosts the zone. Obtain the TSIG key for the DNS nameservers (clients) that you want to add to the BIG-IP system configuration.

Note: *TSIG keys are created by a third party tool such as BIND's* `keygen` *utility.*

When you want the BIG-IP system to authenticate the identity of the DNS server and DNS nameservers (clients) when communicating about DNS zone transfers, add TSIG keys to the BIG-IP system configuration.

1. On the Main tab, click **DNS** > **Delivery** > **Keys** > **TSIG Key List**.
   The TSIG Key List screen opens.
2. Click **Create**.
   The New TSIG Key screen opens.
3. In the **Name** field, type the name of the TSIG key.
4. From the Algorithm list, select the algorithm that was used to generate the key.
5. In the **Secret** field, type the TSIG key secret.
6. Click **Finished**.
7. Create additional TSIG keys, as needed.

Add the server TSIG key for the DNS server to the DNS zone configured on the BIG-IP system. Add TSIG keys to DNS nameservers (clients) configured on the BIG-IP system.

Adding DNS nameserver (client) objects

Gather the IP addresses of the DNS nameservers (clients) from which the BIG-IP® system accepts zone transfer requests for a DNS zone. Optional: Ensure that the client TSIG key is available on the BIG-IP system.

To allow DNS nameservers (clients) to request zone transfers for a zone, add a nameserver object that represents each client. Optionally, you can add a client TSIG key that the BIG-IP system uses to authenticate the identity of the client during zone transfer communications.

1. On the Main tab, click **DNS** > **Delivery** > **Nameservers**.
   The Nameservers List screen opens.
2. Click **Create**.
   The New Nameserver screen opens.
3. In the **Name** field, type a name for the DNS nameserver (client).
4. In the **Address** field, type the IP address on which the DNS nameserver (client) listens for DNS messages.
5. Optional: From the **TSIG Key** list, select the TSIG key that matches the TSIG key on the DNS nameserver (client).

   The BIG-IP system uses this TSIG key to authenticate zone transfer communications as coming from this client and to sign communications sent to this client.
6. Click **Finished**.
7. Add nameserver objects to represent other DNS nameservers (clients).

Add the DNS nameservers (clients) objects to the **Zone Transfer Client** list of the DNS zone on the BIG-IP system.

Enabling zone transfers

To enable the BIG-IP system to handle zone transfers, create a custom DNS profile.

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. Name the profile `dns_zxfr`.
4. Select the **Custom** check box.
5. From the **DNS Express** list, select **Disabled**.
6. From the **Zone Transfer** list, select **Enabled**.
7. From the **Unhandled Query Actions** list, select **Allow**.
   The BIG-IP system forwards zone transfer requests to a DNS server or a member of a pool of DNS servers.
8. From the **Use BIND Server on BIG-IP** list, select **Disabled**.
9. Click **Finished**.

Assign the profile to listeners.

Creating a DNS zone

Before you create a DNS zone to serve as a proxy for a zone hosted on a DNS server on your network, do the following:

- Optional: Ensure that the TSIG key on the DNS server is available on the BIG-IP system.
- Determine the name you want to use for the DNS zone. The name must exactly match the name on the DNS server that hosts the zone.

Note: *Zone names are case insensitive.*

When you want the BIG-IP system to act as a proxy for a zone hosted on a DNS server on your network, create a DNS zone and associate the server TSIG key on the DNS server with the zone on the BIG-IP system.

1. On the Main tab, click **DNS** > **Zones**.
   The Zone List screen opens.
2. Click **Create**.
   The New Zone screen opens.
3. In the **Name** field, type the name of the DNS zone.

   The name must begin and end with a letter and contain only letters, numbers, and the period and hyphen (-) characters.
4. In the Zone Transfer Clients area, move the nameservers that can initiate zone transfers from the **Available** list to the **Active** list.
5. Optional: From the **Server Key** list, select the TSIG key that matches the TSIG key on the DNS server.

   The BIG-IP system uses this TSIG key to sign DNS zone transfer requests, before forwarding the requests to the DNS server that hosts this zone, and then to verify a zone transfer returned from the DNS server.
6. Click **Finished**.

Creating listeners to forward zone transfer requests

Determine to which DNS server you want the listeners to forward DNS zone transfer requests.

Create listeners to alert the BIG-IP® system to zone transfer requests destined for a DNS server that hosts the zone. Create two listeners that use the TCP protocol, one each for an IPv4 address and IPv6 address.

Note: *DNS zone transfers use TCP port 53.*

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 **Create**.
   The Listeners properties screen opens.
3. In the **Name** field, type a unique name for the listener.
4. For the Destination setting, in the **Address** field, type the IPv4 address on which the BIG-IP system listens for DNS zone transfer requests for a zone hosted on a DNS server.
5. From the **Listener** list, select **Advanced**.
6. From the **VLAN Traffic** list, select **All VLANs**.
7. Optional: If you are using SNATs on your network, from the **Source Address Translation** list, select **SNAT**.
8. Optional: If you are using NATs on your network, for the **Address Translation** setting, select the **Enabled** check box.
9. Optional: If you are using port translation on your network, for the **Port Translation** setting, select the **Enabled** check box.
10. In the Service area, from the **DNS Profile** list, select **dns_zxfr** (the custom profile you created to enable the BIG-IP system to process zone transfer requests).
11. In the Service area, from the **Protocol** list, select **TCP**.
12. Click **Repeat**.
13. Create another listener with the same settings, except using an IPv6 address.
14. Click **Finished**.

Creating virtual servers to forward zone transfer requests

Determine to which DNS server you want the virtual servers to forward DNS zone transfer requests.

Create virtual servers to alert the BIG-IP system to zone transfer requests destined for a DNS server that hosts the zone. Create two virtual servers that use the TCP protocol, one each for an IPv4 address and IPv6 address.

Note: *DNS zone transfers use port 53.*

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 **Create** button.

The New Virtual Server screen opens.

3. In the **Name** field, type a unique name for the virtual server.
4. For the **Destination** setting, in the **Address** field, type the IP address you want to use for the virtual server.
5. In the **Service Port** field, type **53**.
6. From the **Protocol** list, select **TCP**.
7. Optional: If you are using SNATs on your network, from the **Source Address Translation** list, select **SNAT**.
8. Optional: From the **SNAT pool** list, select the name of an existing SNAT pool.
9. From the **Configuration** list, select **Advanced**.
10. From the **DNS Profile** list, select the custom DNS profile you created.
11. Click **Finished**.

Create another virtual server with the TCP protocol, but use an IPv6 address and configuration.

Chapter 3

Configuring BIG-IP to Load Balance Zone Transfer Requests to a Pool of DNS Servers

Overview: Configuring BIG-IP to load balance zone transfer requests to a pool of DNS servers

Within your network, the BIG-IP® system can act as a proxy for a pool of DNS servers hosting a zone. In this case, when a DNS nameserver (client) in a specified list of servers sends a zone transfer request, the BIG-IP system load balances the request to a pool of DNS servers that host the zone. A pool member responds with a zone transfer, and the BIG-IP system sends the zone transfer to the client that made the zone transfer request. Optionally, the BIG-IP system can use transaction signature (TSIG) keys to validate the identity of the pool member sending a zone transfer and the DNS nameservers (clients) sending zone transfer requests.

Example of load balancing zone transfer requests with client-side TSIG authentication to a pool

In this figure, an administrator at Site Request configures the BIG-IP system to load balance zone transfer requests for siterequest.com to a pool of DNS servers and uses TSIG key authentication only on the client-side.

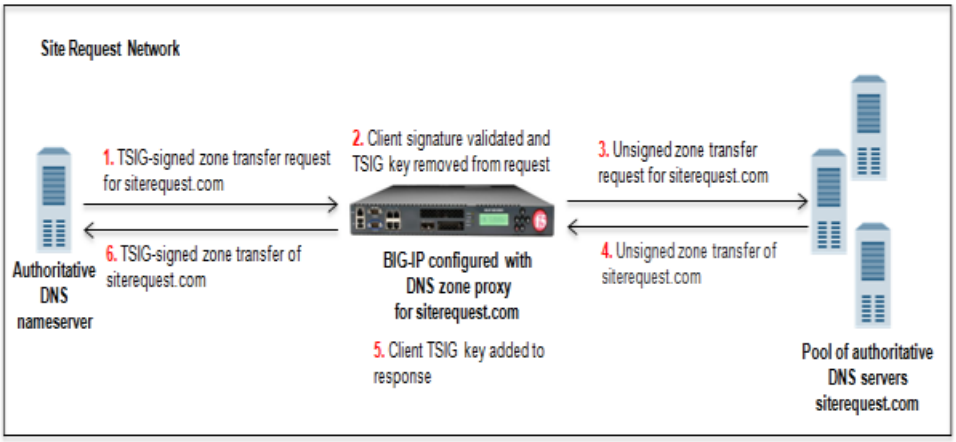


Figure 6: BIG-IP system load balancing zone transfer requests to a pool of DNS servers with client-side TSIG authentication

1. DNS nameserver (client) sends TSIG-signed zone transfer request.
2. BIG-IP system validates the signature and removes the client TSIG key from the request.
3. BIG-IP system sends unsigned zone transfer request to a member of a pool of DNS servers that host the zone.
4. Pool member answers with an unsigned zone transfer to the BIG-IP system.
5. BIG-IP system signs the response with the client TSIG key.
6. BIG-IP system sends the TSIG-signed zone transfer to the DNS nameserver (client).

Example of load balancing zone transfer requests with client-side and server-side TSIG authentication to a pool

In this figure, an administrator at Site Request configures the BIG-IP® system to load balance zone transfer requests for `siterequest.com` to a pool of DNS servers, and uses TSIG key authentication on both the client- and server-sides.

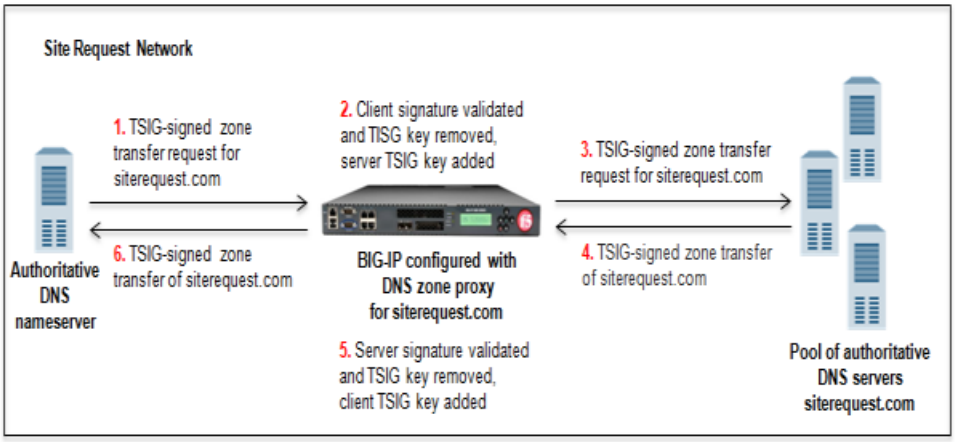


Figure 7: BIG-IP system load balancing zone transfer requests to a pool of DNS servers using client-side TSIG authentication

1. DNS nameserver (client) sends TSIG-signed zone transfer request.
2. BIG-IP system validates the signature, removes the client TSIG key from the request, and then adds the server TSIG key to the request.
3. BIG-IP system sends the TSIG-signed request to a member of the pool of DNS servers that host the zone.
4. Pool member answers with a TSIG-signed zone transfer to the BIG-IP system.
5. BIG-IP system validates the signature, removes the server TSIG key from the response, and signs the response with the client TSIG key.
6. BIG-IP system sends the TSIG-signed zone transfer to the DNS nameserver (client).

About TSIG key authentication

The BIG-IP® system can use transaction signature (TSIG) keys to authenticate communications about zone transfers between the BIG-IP system and authoritative DNS servers, and between the BIG-IP system and DNS nameservers (clients). TSIG keys are generated by a third party tool such as BIND's keygen utility. Using TSIG keys is optional.

TSIG key configured on authoritative DNS server

You can add a TSIG key to a nameserver object that represents an authoritative DNS server. With this configuration, when the DNS server sends a NOTIFY message to the BIG-IP system, DNS Express™ responds with a TSIG-signed zone transfer request. Then the DNS server returns a TSIG-signed zone transfer. If required, you can disable the **Verify Notify TSIG** option on the DNS zone. With this configuration, DNS Express can process a NOTIFY message without a TSIG key, even when a subsequent zone transfer requires a TSIG key.

TSIG key configured on DNS nameserver (client)

You can add a TSIG key to a nameserver object that represents a DNS nameserver (client). When the client sends a TSIG-signed zone transfer request, DNS Express returns a TSIG-signed zone transfer.

TSIG key configured on DNS zone

You can add a server TSIG key to a DNS zone on the BIG-IP system. With this configuration, the system uses this TSIG key when the zone on the BIG-IP system is a proxy for the zone on the server. There are two possible scenarios:

- Client sends TSIG-signed zone transfer request

  When the BIG-IP system receives a TSIG-signed zone transfer request from a client for a DNS zone for which it is a proxy, the system validates the client TSIG key and removes the key from the request. The system then adds the server TSIG key to the request and forwards the TSIG-signed request to the DNS server or load balances the TSIG-signed request to a pool of DNS servers. The DNS server responds with a TSIG-signed zone transfer. The BIG-IP system validates the server TSIG key and removes the key. Then the system adds the client TSIG key and returns a TSIG-signed signed zone transfer to the client.

- Client sends unsigned zone transfer request

  When the BIG-IP system receives an unsigned zone transfer request from a client for a DNS zone for which it is a proxy, the system adds the server TSIG key to the request. The system then forwards the TSIG-signed request to the DNS server or load balances the TSIG-signed request to a pool of DNS servers. The DNS server responds with a TSIG-signed zone transfer. The BIG-IP system validates the server TSIG key and removes the key. Then the system returns an unsigned zone transfer to the client.

About listeners

A *listener* is a specialized virtual server that passively checks for DNS packets on port 53 and the IP address you assign to the listener. When a DNS request is sent to the IP address of the listener, the BIG-IP® system either handles the request or forwards the request to the appropriate resource.

Task summary

Perform these tasks to configure a DNS zone on the BIG-IP system that is a proxy for a pool of DNS servers hosting a DNS zone in your network:

Configuring BIG-IP to Load Balance Zone Transfer Requests to a Pool of DNS Servers
Configuring BIND servers to allow zone transfers
Adding TSIG keys
Adding DNS nameserver (client) objects
Enabling zone transfers
Creating a custom DNS monitor
Creating a pool of local DNS servers for load balancing zone transfer requests
Creating a DNS zone
Creating listeners to load balance zone transfer requests to a pool of DNS servers
Creating virtual servers to load balance zone transfer requests to a pool of DNS servers

Configuring BIND servers to allow zone transfers

If you are unfamiliar with how to modify BIND server files, review the fifth edition of *DNS and BIND*, available from O'Reilly Media.

Typically, BIND servers allow zone transfers to any DNS nameserver requesting a zone transfer. That is, `named.conf` on a typical BIND server does not contain an allow-transfer statement. Therefore, adding an allow-transfer statement to a BIND server actually restricts zone transfers to a specified list of DNS nameservers.

When you want the BIG-IP® system to act as a proxy for a DNS zone configured on a BIND server, you must add an *allow-transfer* statement to `named.conf` on the BIND server that hosts the zone.

Here is an example allow-transfer statement that you can modify to meet your needs: `allow-transfer { localhost; <self IP address on BIG-IP from which zone transfer request is sent to the DNS server>; };`

```
allow-transfer { localhost; 10.10.10.1 ; };
```

Adding TSIG keys

Obtain the TSIG key that the DNS servers in the pool that hosts the zone use to authenticate zone transfer requests. Optionally, obtain the TSIG key for the DNS nameserver (client) that you want to add to the BIG-IP system configuration.

Note: *TSIG keys are created by a third party tool such as BIND's keygen utility. The configuration of each DNS server in the pool must contain the same TSIG key.*

When you want the BIG-IP system to validate zone transfers from a pool DNS servers, add the server TSIG key to the BIG-IP system configuration. Optionally, if you want the BIG-IP system to validate the DNS nameservers (clients) sending zone transfer requests, add the client TSIG keys.

1. On the Main tab, click **DNS** > **Delivery** > **Keys** > **TSIG Key List**.
   The TSIG Key List screen opens.
2. Click **Create**.
   The New TSIG Key screen opens.
3. In the **Name** field, type the name of the TSIG key.
4. From the Algorithm list, select the algorithm that was used to generate the key.
5. In the **Secret** field, type the TSIG key secret.
6. Click **Finished**.
7. If the DNS nameservers (clients) requesting zone transfers contain a TSIG key, repeat steps 2-7 to add each client TSIG key.

Add the server TSIG key to a DNS zone configured on the BIG-IP system. Optionally, add TSIG keys to DNS nameservers (clients) configured on the BIG-IP system.

Adding DNS nameserver (client) objects

Gather the IP addresses of the DNS nameservers (clients) from which the BIG-IP® system accepts zone transfer requests for a DNS zone. Optional: Ensure that the client TSIG key is available on the BIG-IP system.

To allow DNS nameservers (clients) to request zone transfers for a zone, add a nameserver object that represents each client. Optionally, you can add a client TSIG key that the BIG-IP system uses to authenticate the identity of the client during zone transfer communications.

1. On the Main tab, click **DNS** > **Delivery** > **Nameservers**.
   The Nameservers List screen opens.
2. Click **Create**.
   The New Nameserver screen opens.
3. In the **Name** field, type a name for the DNS nameserver (client).
4. In the **Address** field, type the IP address on which the DNS nameserver (client) listens for DNS messages.
5. Optional: From the **TSIG Key** list, select the TSIG key that matches the TSIG key on the DNS nameserver (client).

   The BIG-IP system uses this TSIG key to authenticate zone transfer communications as coming from this client and to sign communications sent to this client.
6. Click **Finished**.
7. Add nameserver objects to represent other DNS nameservers (clients).

Add the DNS nameservers (clients) objects to the **Zone Transfer Client** list of the DNS zone on the BIG-IP system.

Enabling zone transfers

To enable the BIG-IP system to handle zone transfers, create a custom DNS profile.

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. Name the profile `dns_zxfr`.
4. Select the **Custom** check box.
5. From the **DNS Express** list, select **Disabled**.
6. From the **Zone Transfer** list, select **Enabled**.
7. From the **Unhandled Query Actions** list, select **Allow**.
   The BIG-IP system forwards zone transfer requests to a DNS server or a member of a pool of DNS servers.
8. From the **Use BIND Server on BIG-IP** list, select **Disabled**.
9. Click **Finished**.

Assign the profile to listeners.

Creating a custom DNS monitor

Create a custom DNS monitor to send DNS queries, generated using the settings you specify, to a pool of DNS servers and validate the DNS responses.

Important: *When defining values for custom monitors, make sure you avoid using any values that are on the list of reserved keywords. For more information, see SOL 3653 (for version 9.0 systems and later) on the AskF5™ technical support web site at* `www.askf5.com`.

---

1. On the Main tab, click **DNS** > **Delivery** > **Load Balancing** > **Monitors** or **Local Traffic** > **Monitors**.
   The Monitor List screen opens.
2. Click **Create**.
   The New Monitor screen opens.
3. Type a name for the monitor in the **Name** field.
4. From the **Type** list, select **DNS**.
5. In the **Query Name** field, type the domain name that you want the monitor to query.
   For the zone, `siterequest.com`, you might want the monitor to query for `www.siterequest.com`.
6. Configure additional settings based on your network requirements.
7. Click **Finished**.

Creating a pool of local DNS servers for load balancing zone transfer requests

Ensure that at least one custom DNS monitor exists on the BIG-IP® system. Gather the IP addresses of the DNS servers that you want to include in a pool to which the BIG-IP® system load balances DNS zone transfer requests.

Create a pool of local DNS servers when you want the BIG-IP system to load balance DNS zone transfer requests to members of the pool.

1. On the Main tab, click **DNS** > **Delivery** > **Load Balancing** > **Pools** or **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 custom DNS monitor you created, and click **<<** to move the monitor to the **Active** list.
5. Add each DNS server that you want to include in the pool using the **New Members** setting:
   a) In the **Address** field, type the IP address of the DNS server.
   b) Type `53` in the **Service Port** field.
   c) (Optional) Type a priority number in the **Priority** field.
   d) Click **Add**.
6. Click **Finished**.

Creating a DNS zone

Before you create a DNS zone to serve as a proxy for a zone hosted on a pool of DNS servers on your network, do the following:

- Ensure that the TSIG key on the DNS server is available on the BIG-IP® system.
- Optionally, ensure that TSIG keys on the DNS nameservers (clients) that can request zone transfers are available on the BIG-IP system.
- Determine the name you want to use for the DNS zone. The name must exactly match the name of the zone on the members of the pool of DNS servers that host the zone.

Note: *Zone names are case insensitive.*

When you want the BIG-IP system to act as a proxy for a zone hosted on a pool of DNS servers on your network, create a DNS zone and associate the server TSIG key on the DNS servers with the zone on the BIG-IP system. Optionally, you can add the dNS nameservers (clients) that can request zone transfers for the zone.

1. On the Main tab, click **DNS** > **Zones**.
   The Zone List screen opens.
2. Click **Create**.
   The New Zone screen opens.
3. In the **Name** field, type the name of the DNS zone.

   The name must begin and end with a letter and contain only letters, numbers, and the period and hyphen (-) characters.
4. In the Zone Transfer Clients area, move the nameservers that can initiate zone transfers from the **Available** list to the **Active** list.
5. Optional: From the **Server Key** list, select the TSIG key that matches the TSIG key on the members of the pool of DNS servers that host this zone.

   The BIG-IP system uses this TSIG key to sign DNS zone transfer requests, before forwarding the requests to a member of the pool of DNS servers that host this zone, and then to verify a zone transfer returned from a member of the pool.

Creating listeners to load balance zone transfer requests to a pool of DNS servers

Determine to which DNS servers you want the listeners to load balance DNS zone transfer requests.

Create listeners to alert the BIG-IP® system to zone transfer requests destined for a pool of DNS servers that host the zone. Create two listeners that use the TCP protocol, one each for an IPv4 address and IPv6 address.

Note: *DNS zone transfers use TCP port 53.*

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 **Create**.
   The Listeners properties screen opens.

3. In the **Name** field, type a unique name for the listener.
4. For the Destination setting, in the **Address** field, type the IPv4 address on which the BIG-IP system listens for DNS zone transfer requests for a zone hosted on pool of DNS servers.
5. From the **Listener** list, select **Advanced**.
6. From the **VLAN Traffic** list, select **All VLANs**.
7. Optional: If you are using SNATs on your network, from the **Source Address Translation** list, select **SNAT**.
8. Optional: If you are using NATs on your network, for the **Address Translation** setting, select the **Enabled** check box.
9. Optional: If you are using port translation on your network, for the **Port Translation** setting, select the **Enabled** check box.
10. In the Service area, from the **Protocol** list, select **TCP**.
11. In the Service area, from the **DNS Profile** list, select **dns_zxfr** (the custom profile you created to enable the BIG-IP system to process zone transfer requests).
12. On the menu bar, click **Load Balancing**.
13. From the **Default Pool** list, select the pool to which this listener forwards DNS zone transfer requests.
14. Click **Repeat**.
15. Create another listener with the same settings, except using a different name and an IPv6 address.
16. Click **Finished**.

Creating virtual servers to load balance zone transfer requests to a pool of DNS servers

Determine to which DNS servers you want the virtual servers to load balance DNS zone transfer requests.

Create virtual servers to alert the BIG-IP system to zone transfer requests destined for a pool of DNS servers that host the zone. Create two virtual servers that use the TCP protocol, one each for an IPv4 address and IPv6 address.

Note: *DNS zone transfers use TCP port* `53`*.*

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 **Create** button.
   The New Virtual Server screen opens.
3. In the **Name** field, type a unique name for the virtual server.
4. For the **Destination** setting, in the **Address** field, type the IP address you want to use for the virtual server.
5. In the **Service Port** field, type **53**.
6. From the **Protocol** list, select **UDP**.
7. Optional: If you are using SNATs on your network, from the **Source Address Translation** list, select **SNAT**.
8. Optional: From the **SNAT pool** list, select the name of an existing SNAT pool.
9. From the **Configuration** list, select **Advanced**.
10. From the **DNS Profile** list, select the custom DNS profile you created.
11. Click **Finished**.

Create another virtual server with the TCP protocol, but use an IPv6 address and configuration.

Chapter 4

Configuring DNSSEC

Introducing DNSSEC

About DNSSEC

Domain Name System Security Extensions (DNSSEC) is an industry-standard protocol that functions as an extension to the Domain Name System (DNS) protocol. BIG-IP® Global Traffic Manager™ (GTM™) uses DNSSEC to guarantee the authenticity of DNS responses, including zone transfers, and to return Denial of Existence responses thus protecting your network against DNS protocol and DNS server attacks.

About DNSSEC keys

BIG-IP® Global Traffic Manager™ (GTM™) uses two types of DNSSEC keys to return DNSSEC-compliant responses: a *zone-signing key* to sign all of the records in a DNSSEC resource record set, and a *key-signing* key to sign only the DNSKEY record (that is the zone-signing key) of a DNSSEC record set.

About enhancing DNSSEC key security

To enhance DNSSEC key security, when automatic key management is configured, BIG-IP® Global Traffic Manager™ (GTM™) uses an automatic key rollover process that uses overlapping generations of a key to ensure that BIG-IP GTM can always respond to queries with DNSSEC-compliant responses. BIG-IP GTM dynamically creates new generations of each key based on the values of the **Rollover Period** and **Expiration Period** of the key.

The first generation of a key has an ID of 0 (zero). Each time BIG-IP GTM dynamically creates a new generation of a key, the ID increments by one. Over time, each generation of a key overlaps the previous generation of the key ensuring that GTM can respond to a DNSSEC query even if one generation of a key becomes unavailable. When a generation of a key expires, BIG-IP GTM automatically removes that generation of the key from the configuration. The value of the **TTL (time-to-live)** of a key specifies how long a client resolver can cache the key.

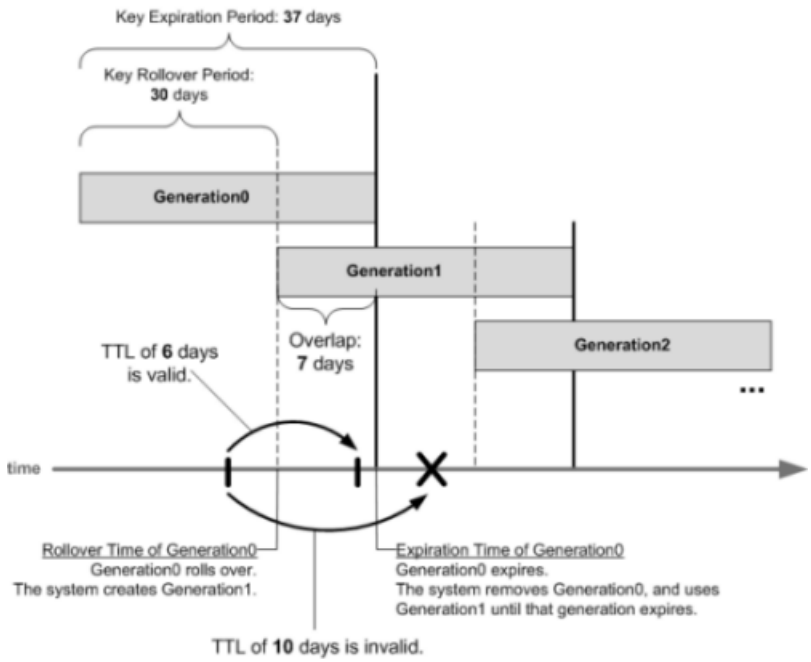


Figure 8: Overlapping generations of a key

How do I prepare for a manual rollover of a DNSSEC key?

When you create DNSSEC key-signing keys and DNSSEC zone-signing keys, it is important to create a disabled standby version of each key that has a similar name. When you associate both pairs of keys with the same zone, you can easily perform a manual rollover of the keys, should an enabled key become compromised.

About SEP records and DNSSEC

Each DNSSEC zone has a list of read-only Security Entry Point (SEP) records. The BIG-IP® Global Traffic Manager™ (GTM™) creates these records automatically when you create a zone. These SEP records consist of Delegation Signer (DS) and DNSKEY records.

Obtaining a trust or DLV anchor

Determine the signed zones from which you want to obtain a trust or DLV anchor.

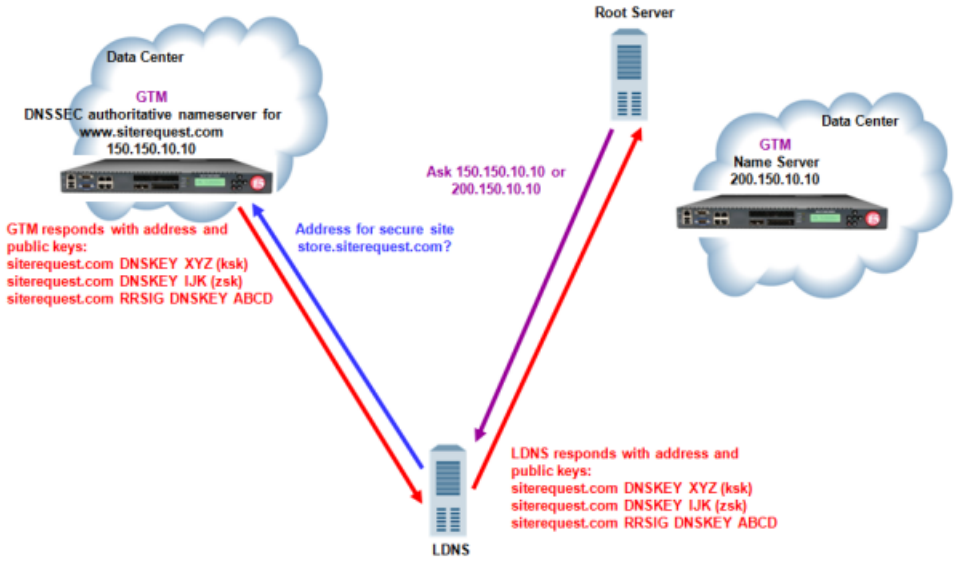
If you want the BIG-IP® system to cache a validated response for the signed zones, you need to obtain a trust or DLV anchor.

1. On the Main tab, click **DNS** > **Zones** > **DNSSEC Zones**.
   The DNSSEC Zone List screen opens.
2. Click the name of the DNSSEC zone for which you want to view or copy SEP records.
3. On the menu bar, click **SEP Records**.
   The SEP records display for each generation of a key. If the SEP record screen is unexpectedly blank, ensure that at least one data center and a server representing the BIG-IP GTM device exist in the BIG-IP system configuration.
4. Copy the trust or DLV anchor from the **DNSKEY Record** field.

About configuring DNSSEC

You can use BIG-IP® Global Traffic Manager™ (GTM™) to ensure that all responses to DNS-related traffic comply with the DNSSEC security protocol. To configure DNSSEC compliance, you create DNSSEC key-signing and zone-signing keys and a DNSSEC zone. Then you assign at least one enabled key-signing key and one enabled zone-signing key to the zone.

Figure 9: Traffic flow when GTM is the DNSSEC authoritative nameserver



About configuring basic DNSSEC

You can secure the DNS traffic handled by BIG-IP® GTM™ using the DNSSEC protocol.

Important: *Before you configure DNSSEC, ensure that at least one data center and a server representing the BIG-IP GTM device exist in the BIG-IP system configuration.*

Task summary

Perform these tasks to configure DNSSEC on GTM.

Creating listeners to identify DNS traffic
Creating automatically managed DNSSEC zone-signing keys
Creating manually managed DNSSEC zone-signing keys
Creating automatically managed DNSSEC key-signing keys
Creating manually managed DNSSEC key-signing keys
Creating a DNSSEC zone
Confirming that GTM is signing DNSSEC records

Creating listeners to identify DNS traffic

Create listeners to identify the DNS traffic that BIG-IP® GTM™ handles. The best practice is to create four listeners: one with an IPv4 address that handles UDP traffic, and one with the same IPv4 address that handles TCP traffic; one with an IPv6 address that handles UDP traffic, and one with the same IPv6 address that handles TCP traffic.

Note: *DNS zone transfers use TCP port* `53`*. If you do not configure listeners for TCP the client might receive the error:* `connection refused or TCP RSTs.`

If you have multiple GTM systems in a device group, perform these steps on only one system.

1. On the Main tab, click **DNS** > **Delivery** > **Listeners**.
   The Listeners List screen opens.
2. Click **Create**.
   The Listeners properties screen opens.
3. In the **Name** field, type a unique name for the listener.
4. For the Destination setting, in the **Address** field, type an IPv4 address on which GTM listens for network traffic.
5. In the Service area, from the **Protocol** list, select **UDP**.
6. Click **Finished**.

Create another listener with the same IPv4 address and configuration, but select **TCP** from the **Protocol** list. Then, create two more listeners, configuring both with the same IPv6 address, but one with the UDP protocol and one with the TCP protocol.

Creating automatically managed DNSSEC zone-signing keys

Ensure that the time setting on BIG-IP® GTM™ is synchronized with the NTP servers on your network. This ensures that each GTM in a synchronization group is referencing the same time when generating keys.

Determine the values you want to configure for the rollover period, expiration period, and TTL of the keys, using the following criteria:

- The amount of time required to send the DS records for the zone to which this key is associated to the organization that manages the parent zone.
- The value of the rollover period must be greater than half the value of the expiration period, as well as less than the value of the expiration period.
- The difference between the values of the rollover and expiration periods must be more than the value of the TTL.

Note: *The values recommended in this procedure are based on the values in the NIST Secure Domain Name System (DNS) Deployment Guide.*

Create automatically-managed zone-signing keys for GTM to use in the DNSSEC authentication process.

1. On the Main tab, click **DNS** > **Delivery** > **Keys** > **DNSSEC Key List**.
   The DNSSEC Key List screen opens.
2. Click **Create**.
   The New DNSSEC Key screen opens.
3. In the **Name** field, type a name for the key.
   Zone names are limited to `63` characters.

4. From the **Type** list, select **Zone Signing Key**.
5. From the **State** list, select **Enabled**.
6. From the **Hardware Security Module** list, select **None**.
7. From the **Algorithm** list, select the digest algorithm the system uses to generate the key signature. Your options are **RSA/SHA1**, **RSA/SHA256**, and **RSA/SHA512**.
8. From the **Key Management** list, select **Automatic**.
   The Key Settings area displays fields for key configuration.
9. In the **Bit Width** field, type `1024`.
10. In the **TTL** field, accept the default value of `86400` (the number of seconds in one day.)

    This value specifies how long a client resolver can cache the key. This value must be less than the difference between the values of the rollover and expiration periods of the key; otherwise, a client can make a query and the system can send a valid key that the client cannot recognize.
11. For the Rollover Period setting, in the **Days** field, type `21`.
12. For the Expiration Period setting, in the **Days** field, type `30`.

    Zero seconds indicates not set, and thus the key does not expire.
13. For the Signature Validity Period setting, accept the default value of seven days.

    This value must be greater than the value of the signature publication period.

    Zero seconds indicates not set, and thus the server verifying the signature never succeeds, because the signature is always expired.
14. For the Signature Publication Period setting, accept the default value of four days and 16 hours.

    This value must be less than the value of the signature validity period.

    Zero seconds indicates not set, and thus the signature is not cached.
15. Click **Finished**.
16. To create a standby key for emergency rollover purposes, repeat these steps using a similar name, and select **Disabled** from the **State** list.

Creating manually managed DNSSEC zone-signing keys

Ensure that the time setting on BIG-IP® GTM™ is synchronized with the NTP servers on your network. This ensures that each GTM in a synchronization group is referencing the same time when generating keys.

When you plan to manually create keys, install the certificate and key pairs on the BIG-IP system, before you attempt to create DNSSEC keys.

Important: *Certificate and key file pairs must have the same name, for example,* `exthsm.crt` *and* `exthsm.key`*.*

Create manually-managed zone-signing keys for GTM to use in the DNSSEC authentication process.

1. On the Main tab, click **DNS** > **Delivery** > **Keys** > **DNSSEC Key List**.
   The DNSSEC Key List screen opens.
2. Click **Create**.
   The New DNSSEC Key screen opens.
3. In the **Name** field, type a name for the key.

   Zone names are limited to `63` characters.
4. From the **Type** list, select **Zone Signing Key**.
5. From the **State** list, select **Enabled**.

6. From the **Hardware Security Module** list, select **None**.
7. From the **Algorithm** list, select the digest algorithm the system uses to generate the key signature. Your options are **RSA/SHA1**, **RSA/SHA256**, and **RSA/SHA512**.
8. From the **Key Management** list, select **Manual**.
   The Key Settings area displays **Certificate** and **Private Key** lists.
9. In the Key Settings area, select a certificate/key pair:
   a) From the **Certificate** list, select a certificate.
   b) From the **Private Key** list, select the key that matches the certificate you selected.
10. Click **Finished**.
11. To create a standby key for emergency rollover purposes, repeat these steps using a similar name, and select **Disabled** from the **State** list.

Creating automatically managed DNSSEC key-signing keys

Ensure that the time setting on BIG-IP® GTM™ is synchronized with the NTP servers on your network. This ensures that each GTM in a synchronization group is referencing the same time when generating keys.

Determine the values you want to configure for the rollover period, expiration period, and TTL of the keys, using the following criteria:

- The amount of time required to send the DS records for the zone to which this key is associated to the organization that manages the parent zone.
- The value of the rollover period must be greater than half the value of the expiration period, as well as less than the value of the expiration period.
- The difference between the values of the rollover and expiration periods must be more than the value of the TTL.

Note: *The values recommended in these steps are based on the values in the NIST Secure Domain Name System (DNS) Deployment Guide.*

Create key-signing keys for GTM to use in the DNSSEC authentication process.

1. On the Main tab, click **DNS** > **Delivery** > **Keys** > **DNSSEC Key List**.
   The DNSSEC Key List screen opens.
2. Click **Create**.
   The New DNSSEC Key screen opens.
3. In the **Name** field, type a name for the key.
   Zone names are limited to `63` characters.
4. From the **Type** list, select **Key Signing Key**.
5. From the **State** list, select **Enabled**.
6. From the **Hardware Security Module** list, select **None**.
7. From the **Algorithm** list, select the digest algorithm the system uses to generate the key signature. Your options are **RSA/SHA1**, **RSA/SHA256**, and **RSA/SHA512**.
8. From the **Key Management** list, select **Automatic**.
   The Key Settings area displays fields for key configuration.
9. In the **Bit Width** field, type `2048`.
10. In the **TTL** field, accept the default value of `86400` (the number of seconds in one day.)

This value specifies how long a client resolver can cache the key. This value must be less than the difference between the values of the rollover and expiration periods of the key; otherwise, a client can make a query and the system can send a valid key that the client cannot recognize.

11. For the Rollover Period setting, in the **Days** field, type `340`.
12. For the Expiration Period setting, in the **Days** field, type `365`.

    Zero seconds indicates not set, and thus the key does not expire.

Tip: *The National Institute of Standards and Technology (NIST) recommends that a key-signing key expire once a year.*

---

13. For the Signature Validity Period setting, accept the default value of seven days.

    This value must be greater than the value of the signature publication period.

    Zero seconds indicates not set, and thus the server verifying the signature never succeeds, because the signature is always expired.
14. For the Signature Publication Period setting, accept the default value of four days and 16 hours.

    This value must be less than the value of the signature validity period.

    Zero seconds indicates not set, and thus the signature is not cached.
15. Click **Finished**.
16. To create a standby key for emergency rollover purposes, repeat these steps using a similar name, and select **Disabled** from the **State** list.

Creating manually managed DNSSEC key-signing keys

Ensure that the time setting on BIG-IP® GTM™ is synchronized with the NTP servers on your network. This ensures that each GTM in a synchronization group is referencing the same time when generating keys.

When you plan to manually create keys, install the certificate and key pairs on the BIG-IP system, before you attempt to create DNSSEC keys.

Important: *Certificate and key file pairs must have the same name, for example,* `exthsm.crt` *and* `exthsm.key`*.*

Create key-signing keys for GTM to use in the DNSSEC authentication process.

1. On the Main tab, click **DNS** > **Delivery** > **Keys** > **DNSSEC Key List**.
   The DNSSEC Key List screen opens.
2. Click **Create**.
   The New DNSSEC Key screen opens.
3. In the **Name** field, type a name for the key.

   Zone names are limited to `63` characters.
4. From the **Type** list, select **Key Signing Key**.
5. From the **State** list, select **Enabled**.
6. From the **Hardware Security Module** list, select **None**.
7. From the **Algorithm** list, select the digest algorithm the system uses to generate the key signature. Your options are **RSA/SHA1**, **RSA/SHA256**, and **RSA/SHA512**.
8. From the **Key Management** list, select **Manual**.
   The Key Settings area displays **Certificate** and **Private Key** lists.
9. In the Key Settings area, select a certificate/key pair:

a) From the **Certificate** list, select a certificate.
b) From the **Private Key** list, select the key that matches the certificate you selected.

10. Click **Finished**.
11. To create a standby key for emergency rollover purposes, repeat these steps using a similar name, and select **Disabled** from the **State** list.

Creating a DNSSEC zone

Before you configure DNSSEC, ensure that at least one data center and a server object representing the BIG-IP® device exist in the BIG-IP system configuration.

Important: *The DNSSEC feature is available only when the BIG-IP system is licensed for BIG-IP Global Traffic Manager™ (GTM™).*

Before the BIG-IP system can sign DNS requests (including zone transfer requests) for a zone using DNSSEC keys, you must create a DNSSEC zone on the system and assign at least one enabled zone-signing and one enabled key-signing key to the zone.

1. On the Main tab, click **DNS** > **Zones** > **DNSSEC Zones**.
   The DNSSEC Zone List screen opens.
2. Click **Create**.
   The New DNSSEC Zone screen opens.
3. In the **Name** field, type a domain name.
   For example, use a zone name of `siterequest.com` to handle DNSSEC requests for `www.siterequest.com` and `*.www.sitrequest.com`.
4. From the **State** list, select **Enabled**.
5. For the **Zone Signing Key** setting, assign at least one enabled zone-signing key to the zone.
   You can associate the same zone-signing key with multiple zones.
6. For the **Key Signing Key** setting, assign at least one enabled key-signing key to the zone.
   You can associate the same key-signing key with multiple zones.
7. Click **Finished**.
   Even if you selected **Enabled** from the **State** list, if there are not at least one zone-signing and one key-signing key in the Active column, the status of the zone changes to offline.

Upload the DS records for this zone to the organization that manages the parent zone. The administrators of the parent zone sign the DS record with their own key and upload it to their zone. You can find the DS records in the Configuration utility.

Confirming that GTM is signing DNSSEC records

After you create DNSSEC zones and zone-signing keys, you can confirm that GTM™ is signing the DNSSEC records.

1. Log on to the command-line interface of a client.
2. At the prompt, type: `dig @<IP address of GTM listener> +dnssec <name of zone>`
   GTM returns the signed RRSIG records for the zone.

About configuring DNSSEC with an external HSM

You can configure BIG-IP® GTM™ to use the DNSSEC protocol to secure the DNS traffic handled by GTM in conjunction with an external HSM system.

Important: *Before you configure DNSSEC, ensure that at least one data center and a server object representing the BIG-IP GTM device exist in the BIG-IP system configuration.*

Task summary

Perform these tasks to configure DNSSEC on GTM.

Creating listeners to identify DNS traffic
Creating automatically managed DNSSEC zone-signing keys for use with an external HSM
Creating manually managed DNSSEC zone-signing keys for use with an external HSM
Creating automatically managed DNSSEC key-signing keys for use with an external HSM
Creating manually managed DNSSEC key-signing keys for use with an external HSM
Creating a DNSSEC zone
Confirming that GTM is signing DNSSEC records

Creating listeners to identify DNS traffic

Create listeners to identify the DNS traffic that BIG-IP® GTM™ handles. The best practice is to create four listeners: one with an IPv4 address that handles UDP traffic, and one with the same IPv4 address that handles TCP traffic; one with an IPv6 address that handles UDP traffic, and one with the same IPv6 address that handles TCP traffic.

Note: *DNS zone transfers use TCP port* `53`*. If you do not configure listeners for TCP the client might receive the error:* `connection refused or TCP RSTs.`

If you have multiple GTM systems in a device group, perform these steps on only one system.

1. On the Main tab, click **DNS** > **Delivery** > **Listeners**.
   The Listeners List screen opens.
2. Click **Create**.
   The Listeners properties screen opens.
3. In the **Name** field, type a unique name for the listener.
4. For the Destination setting, in the **Address** field, type an IPv4 address on which GTM listens for network traffic.
5. In the Service area, from the **Protocol** list, select **UDP**.
6. Click **Finished**.

Create another listener with the same IPv4 address and configuration, but select **TCP** from the **Protocol** list. Then, create two more listeners, configuring both with the same IPv6 address, but one with the UDP protocol and one with the TCP protocol.

Creating automatically managed DNSSEC zone-signing keys for use with an external HSM

Ensure that the time setting on BIG-IP® GTM™ is synchronized with the NTP servers on your network. This ensures that each GTM in a synchronization group is referencing the same time when generating keys.

Determine the values you want to configure for the rollover period, expiration period, and TTL of the keys, using the following criteria:

- The amount of time required to send the DS records for the zone to which this key is associated to the organization that manages the parent zone.
- The value of the rollover period must be greater than half the value of the expiration period, as well as less than the value of the expiration period.
- The difference between the values of the rollover and expiration periods must be more than the value of the TTL.

Note: *The values recommended in this procedure are based on the values in the NIST Secure Domain Name System (DNS) Deployment Guide.*

Create zone-signing keys for GTM to use in the DNSSEC authentication process.

1. On the Main tab, click **DNS** > **Delivery** > **Keys** > **DNSSEC Key List**.
   The DNSSEC Key List screen opens.
2. Click **Create**.
   The New DNSSEC Key screen opens.
3. In the **Name** field, type a name for the key.

   Zone names are limited to `63` characters.
4. From the **Type** list, select **Zone Signing Key**.
5. From the **State** list, select **Enabled**.
6. From the **Hardware Security Module** list, select **External**, if you use a network HSM.
7. From the **Algorithm** list, select the digest algorithm the system uses to generate the key signature. Your options are **RSA/SHA1**, **RSA/SHA256**, and **RSA/SHA512**.
8. From the **Key Management** list, select **Automatic**.
   The Key Settings area displays fields for key configuration.
9. In the **Bit Width** field, type `1024`.
10. In the **TTL** field, accept the default value of `86400` (the number of seconds in one day.)

    This value specifies how long a client resolver can cache the key. This value must be less than the difference between the values of the rollover and expiration periods of the key; otherwise, a client can make a query and the system can send a valid key that the client cannot recognize.
11. For the Rollover Period setting, in the **Days** field, type `21`.
12. For the Expiration Period setting, in the **Days** field, type `30`.

    Zero seconds indicates not set, and thus the key does not expire.
13. For the Signature Validity Period setting, accept the default value of seven days.

    This value must be greater than the value of the signature publication period.

    Zero seconds indicates not set, and thus the server verifying the signature never succeeds, because the signature is always expired.
14. For the Signature Publication Period setting, accept the default value of four days and 16 hours.

    This value must be less than the value of the signature validity period.

    Zero seconds indicates not set, and thus the signature is not cached.

15. Click **Finished**.
16. To create a standby key for emergency rollover purposes, repeat these steps using a similar name, and select **Disabled** from the **State** list.

Creating manually managed DNSSEC zone-signing keys for use with an external HSM

Ensure that the time setting on BIG-IP® GTM™ is synchronized with the NTP servers on your network. This ensures that each GTM in a synchronization group is referencing the same time when generating keys.

When you plan to manually create keys, install the certificate and key pairs on the BIG-IP system, before you attempt to create DNSSEC keys.

Important: *Certificate and key file pairs must have the same name, for example,* `exthsm.crt` *and* `exthsm.key`*.*

Create zone-signing keys for GTM to use in the DNSSEC authentication process.

1. On the Main tab, click **DNS** > **Delivery** > **Keys** > **DNSSEC Key List**.
   The DNSSEC Key List screen opens.
2. Click **Create**.
   The New DNSSEC Key screen opens.
3. In the **Name** field, type a name for the key.
   Zone names are limited to `63` characters.
4. From the **Type** list, select **Zone Signing Key**.
5. From the **State** list, select **Enabled**.
6. From the **Hardware Security Module** list, select **External**, if you use a network HSM.
7. From the **Algorithm** list, select the digest algorithm the system uses to generate the key signature. Your options are **RSA/SHA1**, **RSA/SHA256**, and **RSA/SHA512**.
8. From the **Key Management** list, select **Manual**.
   The Key Settings area displays **Certificate** and **Private Key** lists.
9. In the Key Settings area, select a certificate/key pair:
   a) From the **Certificate** list, select a certificate.
   b) From the **Private Key** list, select the key that matches the certificate you selected.
10. Click **Finished**.
11. To create a standby key for emergency rollover purposes, repeat these steps using a similar name, and select **Disabled** from the **State** list.

Creating automatically managed DNSSEC key-signing keys for use with an external HSM

Ensure that the time setting on BIG-IP® GTM™ is synchronized with the NTP servers on your network. This ensures that each GTM in a synchronization group is referencing the same time when generating keys.

Determine the values you want to configure for the rollover period, expiration period, and TTL of the keys, using the following criteria:

- The amount of time required to send the DS records for the zone to which this key is associated to the organization that manages the parent zone.

- The value of the rollover period must be greater than half the value of the expiration period, as well as less than the value of the expiration period.
- The difference between the values of the rollover and expiration periods must be more than the value of the TTL.

Note: *The values recommended in this procedure are based on the values in the NIST Secure Domain Name System (DNS) Deployment Guide.*

Create key-signing keys for GTM to use in the DNSSEC authentication process.

1. On the Main tab, click **DNS** > **Delivery** > **Keys** > **DNSSEC Key List**.
   The DNSSEC Key List screen opens.
2. Click **Create**.
   The New DNSSEC Key screen opens.
3. In the **Name** field, type a name for the key.

   Zone names are limited to `63` characters.
4. From the **Type** list, select **Key Signing Key**.
5. From the **State** list, select **Enabled**.
6. From the **Hardware Security Module** list, select **External**, if you use a network HSM.
7. From the **Algorithm** list, select the digest algorithm the system uses to generate the key signature. Your options are **RSA/SHA1**, **RSA/SHA256**, and **RSA/SHA512**.
8. From the **Key Management** list, select **Automatic**.
   The Key Settings area displays fields for key configuration.
9. In the **Bit Width** field, type `2048`.
10. In the **TTL** field, accept the default value of `86400` (the number of seconds in one day.)

    This value specifies how long a client resolver can cache the key. This value must be less than the difference between the values of the rollover and expiration periods of the key; otherwise, a client can make a query and the system can send a valid key that the client cannot recognize.
11. For the Rollover Period setting, in the **Days** field, type `340`.
12. For the Expiration Period setting, in the **Days** field, type `365`.

    Zero seconds indicates not set, and thus the key does not expire.

    Tip: *The National Institute of Standards and Technology (NIST) recommends that a key-signing key expire once a year.*

    ---
13. For the Signature Validity Period setting, accept the default value of seven days.

    This value must be greater than the value of the signature publication period.

    Zero seconds indicates not set, and thus the server verifying the signature never succeeds, because the signature is always expired.
14. For the Signature Publication Period setting, accept the default value of four days and 16 hours.

    This value must be less than the value of the signature validity period.

    Zero seconds indicates not set, and thus the signature is not cached.
15. Click **Finished**.
16. To create a standby key for emergency rollover purposes, repeat these steps using a similar name, and select **Disabled** from the **State** list.

Creating manually managed DNSSEC key-signing keys for use with an external HSM

Ensure that the time setting on BIG-IP® GTM™ is synchronized with the NTP servers on your network. This ensures that each GTM in a synchronization group is referencing the same time when generating keys.

When you plan to manually create keys, install the certificate and key pairs on the BIG-IP system, before you attempt to create DNSSEC keys.

Important: *Certificate and key file pairs must have the same name, for example,* `exthsm.crt` *and* `exthsm.key`*.*

Create key-signing keys for GTM to use in the DNSSEC authentication process.

1. On the Main tab, click **DNS** > **Delivery** > **Keys** > **DNSSEC Key List**.
   The DNSSEC Key List screen opens.
2. Click **Create**.
   The New DNSSEC Key screen opens.
3. In the **Name** field, type a name for the key.
   Zone names are limited to `63` characters.
4. From the **Type** list, select **Key Signing Key**.
5. From the **State** list, select **Enabled**.
6. From the **Hardware Security Module** list, select **External**, if you use a network HSM.
7. From the **Algorithm** list, select the digest algorithm the system uses to generate the key signature. Your options are **RSA/SHA1**, **RSA/SHA256**, and **RSA/SHA512**.
8. From the **Key Management** list, select **Manual**.
   The Key Settings area displays **Certificate** and **Private Key** lists.
9. In the Key Settings area, select a certificate/key pair:
   a) From the **Certificate** list, select a certificate.
   b) From the **Private Key** list, select the key that matches the certificate you selected.
10. Click **Finished**.
11. To create a standby key for emergency rollover purposes, repeat these steps using a similar name, and select **Disabled** from the **State** list.

Creating a DNSSEC zone

Before you configure DNSSEC, ensure that at least one data center and a server object representing the BIG-IP® device exist in the BIG-IP system configuration.

Important: *The DNSSEC feature is available only when the BIG-IP system is licensed for BIG-IP Global Traffic Manager™ (GTM™).*

Before the BIG-IP system can sign DNS requests (including zone transfer requests) for a zone using DNSSEC keys, you must create a DNSSEC zone on the system and assign at least one enabled zone-signing and one enabled key-signing key to the zone.

1. On the Main tab, click **DNS** > **Zones** > **DNSSEC Zones**.
   The DNSSEC Zone List screen opens.
2. Click **Create**.

The New DNSSEC Zone screen opens.

3. In the **Name** field, type a domain name.
   For example, use a zone name of `siterequest.com` to handle DNSSEC requests for `www.siterequest.com` and `*.www.sitrequest.com`.
4. From the **State** list, select **Enabled**.
5. For the **Zone Signing Key** setting, assign at least one enabled zone-signing key to the zone.
   You can associate the same zone-signing key with multiple zones.
6. For the **Key Signing Key** setting, assign at least one enabled key-signing key to the zone.
   You can associate the same key-signing key with multiple zones.
7. Click **Finished**.
   Even if you selected **Enabled** from the **State** list, if there are not at least one zone-signing and one key-signing key in the Active column, the status of the zone changes to offline.

Upload the DS records for this zone to the organization that manages the parent zone. The administrators of the parent zone sign the DS record with their own key and upload it to their zone. You can find the DS records in the Configuration utility.

Confirming that GTM is signing DNSSEC records

After you create DNSSEC zones and zone-signing keys, you can confirm that GTM™ is signing the DNSSEC records.

1. Log on to the command-line interface of a client.
2. At the prompt, type: `dig @<IP address of GTM listener> +dnssec <name of zone>`
   GTM returns the signed RRSIG records for the zone.

Configuring DNSSEC with an internal HSM

You can configure BIG-IP® GTM™ to use the DNSSEC protocol to secure the DNS traffic handled by GTM in conjunction with an internal HSM system.

Important: *Before you configure DNSSEC, ensure that at least one data center and a server representing the BIG-IP GTM device exist in the BIG-IP system configuration.*

Task summary

Perform these tasks to configure DNSSEC on GTM.

Creating listeners to identify DNS traffic
Creating automatically managed DNSSEC zone-signing keys for use with an internal HSM
Creating automatically managed DNSSEC key-signing keys for use with an internal HSM
Creating a DNSSEC zone
Confirming that GTM is signing DNSSEC records

Creating listeners to identify DNS traffic

Create listeners to identify the DNS traffic that BIG-IP® GTM™ handles. The best practice is to create four listeners: one with an IPv4 address that handles UDP traffic, and one with the same IPv4 address that handles TCP traffic; one with an IPv6 address that handles UDP traffic, and one with the same IPv6 address that handles TCP traffic.

Note: *DNS zone transfers use TCP port* `53`*. If you do not configure listeners for TCP the client might receive the error:* `connection refused or TCP RSTs.`

If you have multiple GTM systems in a device group, perform these steps on only one system.

1. On the Main tab, click **DNS** > **Delivery** > **Listeners**.
   The Listeners List screen opens.
2. Click **Create**.
   The Listeners properties screen opens.
3. In the **Name** field, type a unique name for the listener.
4. For the Destination setting, in the **Address** field, type an IPv4 address on which GTM listens for network traffic.
5. In the Service area, from the **Protocol** list, select **UDP**.
6. Click **Finished**.

Create another listener with the same IPv4 address and configuration, but select **TCP** from the **Protocol** list. Then, create two more listeners, configuring both with the same IPv6 address, but one with the UDP protocol and one with the TCP protocol.

Creating automatically managed DNSSEC zone-signing keys for use with an internal HSM

Ensure that the time setting on BIG-IP® GTM™ is synchronized with the NTP servers on your network. This ensures that each GTM in a synchronization group is referencing the same time when generating keys.

Determine the values you want to configure for the rollover period, expiration period, and TTL of the keys, using the following criteria:

- The amount of time required to send the DS records for the zone to which this key is associated to the organization that manages the parent zone.
- The value of the rollover period must be greater than half the value of the expiration period, as well as less than the value of the expiration period.
- The difference between the values of the rollover and expiration periods must be more than the value of the TTL.

Note: *The values recommended in this procedure are based on the values in the NIST Secure Domain Name System (DNS) Deployment Guide.*

Create zone-signing keys for GTM to use in the DNSSEC authentication process in conjunction with an internal HSM.

1. On the Main tab, click **DNS** > **Delivery** > **Keys** > **DNSSEC Key List**.
   The DNSSEC Key List screen opens.
2. Click **Create**.
   The New DNSSEC Key screen opens.
3. In the **Name** field, type a name for the key.

Zone names are limited to 63 characters.

4. From the **Type** list, select **Zone Signing Key**.
5. From the **State** list, select **Enabled**.
6. From the **Hardware Security Module** list, select **Internal**, if you use a FIPs internal HSM card.
7. From the **Algorithm** list, select the digest algorithm the system uses to generate the key signature. Your options are **RSA/SHA1**, **RSA/SHA256**, and **RSA/SHA512**.
8. From the **Key Management** list, select **Automatic**.
   The Key Settings area displays fields for key configuration.
9. In the **Bit Width** field, type 1024.
10. In the **TTL** field, accept the default value of 86400 (the number of seconds in one day.)

    This value specifies how long a client resolver can cache the key. This value must be less than the difference between the values of the rollover and expiration periods of the key; otherwise, a client can make a query and the system can send a valid key that the client cannot recognize.
11. For the Rollover Period setting, in the **Days** field, type 21.
12. For the Expiration Period setting, in the **Days** field, type 30.

    Zero seconds indicates not set, and thus the key does not expire.
13. For the Signature Validity Period setting, accept the default value of seven days.

    This value must be greater than the value of the signature publication period.

    Zero seconds indicates not set, and thus the server verifying the signature never succeeds, because the signature is always expired.
14. For the Signature Publication Period setting, accept the default value of four days and 16 hours.

    This value must be less than the value of the signature validity period.

    Zero seconds indicates not set, and thus the signature is not cached.
15. Click **Finished**.
16. To create a standby key for emergency rollover purposes, repeat these steps using a similar name, and select **Disabled** from the **State** list.

Creating automatically managed DNSSEC key-signing keys for use with an internal HSM

Ensure that the time setting on BIG-IP® GTM™ is synchronized with the NTP servers on your network. This ensures that each GTM in a synchronization group is referencing the same time when generating keys.

Determine the values you want to configure for the rollover period, expiration period, and TTL of the keys, using the following criteria:

- The amount of time required to send the DS records for the zone to which this key is associated to the organization that manages the parent zone.
- The value of the rollover period must be greater than half the value of the expiration period, as well as less than the value of the expiration period.
- The difference between the values of the rollover and expiration periods must be more than the value of the TTL.

Note: *The values recommended in this procedure are based on the values in the NIST Secure Domain Name System (DNS) Deployment Guide.*

Create key-signing keys for GTM to use in the DNSSEC authentication process in conjunction with an internal HSM.

1. On the Main tab, click **DNS** > **Delivery** > **Keys** > **DNSSEC Key List**.
   The DNSSEC Key List screen opens.
2. Click **Create**.
   The New DNSSEC Key screen opens.
3. In the **Name** field, type a name for the key.
   Zone names are limited to 63 characters.
4. From the **Type** list, select **Key Signing Key**.
5. From the **State** list, select **Enabled**.
6. From the **Hardware Security Module** list, select **Internal**, if you use a FIPs internal HSM card.
7. From the **Algorithm** list, select the digest algorithm the system uses to generate the key signature. Your options are **RSA/SHA1**, **RSA/SHA256**, and **RSA/SHA512**.
8. From the **Key Management** list, select **Automatic**.
   The Key Settings area displays fields for key configuration.
9. In the **Bit Width** field, type 2048.
10. In the **TTL** field, accept the default value of 86400 (the number of seconds in one day.)
    This value specifies how long a client resolver can cache the key. This value must be less than the difference between the values of the rollover and expiration periods of the key; otherwise, a client can make a query and the system can send a valid key that the client cannot recognize.
11. For the Rollover Period setting, in the **Days** field, type 340.
12. For the Expiration Period setting, in the **Days** field, type 365.
    Zero seconds indicates not set, and thus the key does not expire.

    Tip: *The National Institute of Standards and Technology (NIST) recommends that a key-signing key expire once a year.*

13. For the Signature Validity Period setting, accept the default value of seven days.
    This value must be greater than the value of the signature publication period.
    Zero seconds indicates not set, and thus the server verifying the signature never succeeds, because the signature is always expired.
14. For the Signature Publication Period setting, accept the default value of four days and 16 hours.
    This value must be less than the value of the signature validity period.
    Zero seconds indicates not set, and thus the signature is not cached.
15. Click **Finished**.
16. To create a standby key for emergency rollover purposes, repeat these steps using a similar name, and select **Disabled** from the **State** list.

Creating a DNSSEC zone

Before you configure DNSSEC, ensure that at least one data center and a server object representing the BIG-IP® device exist in the BIG-IP system configuration.

Important: *The DNSSEC feature is available only when the BIG-IP system is licensed for BIG-IP Global Traffic Manager™ (GTM™).*

Before the BIG-IP system can sign DNS requests (including zone transfer requests) for a zone using DNSSEC keys, you must create a DNSSEC zone on the system and assign at least one enabled zone-signing and one enabled key-signing key to the zone.

1. On the Main tab, click **DNS** > **Zones** > **DNSSEC Zones**.
   The DNSSEC Zone List screen opens.
2. Click **Create**.
   The New DNSSEC Zone screen opens.
3. In the **Name** field, type a domain name.

   For example, use a zone name of `siterequest.com` to handle DNSSEC requests for `www.siterequest.com` and `*.www.sitrequest.com`.
4. From the **State** list, select **Enabled**.
5. For the **Zone Signing Key** setting, assign at least one enabled zone-signing key to the zone.

   You can associate the same zone-signing key with multiple zones.
6. For the **Key Signing Key** setting, assign at least one enabled key-signing key to the zone.

   You can associate the same key-signing key with multiple zones.
7. Click **Finished**.
   Even if you selected **Enabled** from the **State** list, if there are not at least one zone-signing and one key-signing key in the Active column, the status of the zone changes to offline.

Upload the DS records for this zone to the organization that manages the parent zone. The administrators of the parent zone sign the DS record with their own key and upload it to their zone. You can find the DS records in the Configuration utility.

Confirming that GTM is signing DNSSEC records

After you create DNSSEC zones and zone-signing keys, you can confirm that GTM™ is signing the DNSSEC records.

1. Log on to the command-line interface of a client.
2. At the prompt, type: `dig @<IP address of GTM listener> +dnssec <name of zone>`
   GTM returns the signed RRSIG records for the zone.

About DNSSEC signing of zone transfers

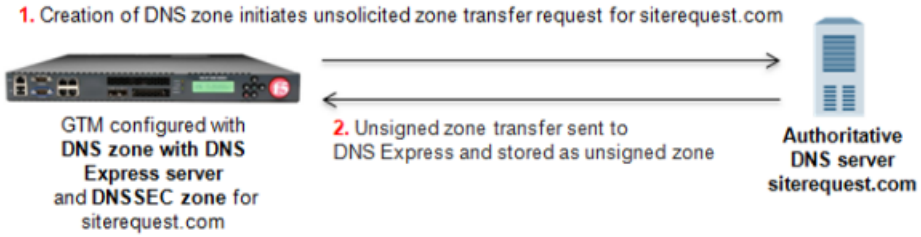
You can configure the BIG-IP® system to sign zone transfers using DNSSEC keys. With this configuration, the DNS nameservers (clients) requesting zone transfers can serve DNSSEC-signed responses to DNS queries.

The BIG-IP system manages the DNSSEC keys and signs the zone transfers even when external HSMs or FIPS cards are used in the configuration. With this configuration, the BIG-IP system must contain a DNSSEC zone with DNSSEC keys and a DNS zone with a list of DNS nameservers (clients) that can request zone transfers for the zone.

Important: *The DNSSEC feature is available only when BIG-IP is licensed for BIG-IP Global Traffic Manager™ (GTM™).*

Example of DNS Express signing zone transfers with DNSSEC keys

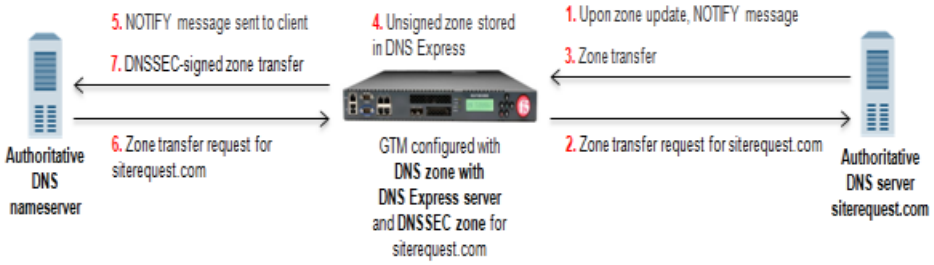
In this figure, a zone is hosted on an authoritative DNS server, that is not secured with DNSSEC keys. An administrator at Site Request creates a DNS zone with a DNS Express™ server and a DNSSEC zone with DNSSEC keys. The name of both zones on the BIG-IP system match the name of the zone on the authoritative DNS server. The creation of the DNS zone initiates an unsigned zone transfer request from DNS Express to the authoritative DNS server that hosts the zone. The server responds with an unsigned zone transfer and the zone is loaded into DNS Express as an unsigned zone.



1. Creation of DNS zone with DNS Express server initiates unsolicited zone transfer request from DNS Express to authoritative DNS server.
2. DNS server responds with unsigned zone transfer to DNS Express, which loads the zone, and stores it as an unsigned zone.

Figure 10: Unsigned DNS zone transfer to DNS Express

In this figure, when the zone is updated, the zone transfer from the server to DNS Express is unsigned. The zone is stored in DNS Express as an unsigned zone. However, when the BIG-IP system receives a zone transfer request, the system signs the zone transfer using DNSSEC keys and sends the signed zone transfer to a DNS nameserver (client).



1. When a zone update occurs, DNS server sends NOTIFY message to DNS Express.
2. DNS Express sends zone transfer request to DNS server.
3. DNS server responds with zone transfer to DNS Express
4. DNS Express stores unsigned zone.
5. DNS Express sends NOTIFY to DNS nameserver client.
6. Client sends zone transfer request to DNS Express.
7. DNS Express responds with DNSSEC-signed zone transfer.

Figure 11: BIG-IP responds to zone transfer request with DNSSEC-signed response

---

Important: *The DNSSEC feature is available only when the BIG-IP system is licensed for BIG-IP Global Traffic Manager™ (GTM™).*

Example of DNS zone proxy with DNSSEC

In this figure, a zone is hosted on an authoritative DNS server, that is not secured with DNSSEC. The BIG-IP® system is configured with both a DNS zone and a DNSSEC zone that match the zone name on the server. The system can forward zone transfer requests to the DNS server, and then sign the response with DNSSEC keys, before sending the response to the client (authoritative DNS nameservers (clients) and cloud providers). This allows the clients and cloud providers to serve DNSSEC-signed DNS queries and responses.

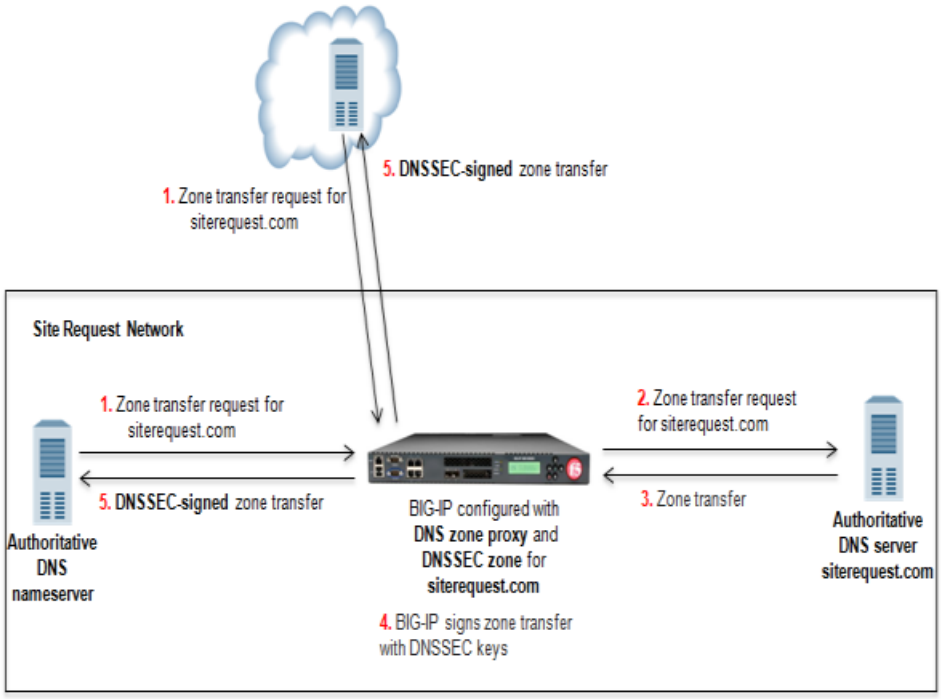


Figure 12: The BIG-IP system configured with DNS zone proxy and DNSSEC zone

1. DNS nameserver (client) sends zone transfer request for a DNS zone.
2. The BIG-IP system forwards the request to the authoritative DNS server.
3. DNS server answers with zone transfer.
4. The BIG-IP system signs the zone transfer with DNSSEC keys.
5. The BIG-IP system sends the DNSSEC-signed zone transfer to the client that made the request.

Important: *The DNSSEC feature is available only when the BIG-IP system is licensed for BIG-IP Global Traffic Manager™ (GTM™).*

Example of BIG-IP load balancing zone transfer request to pool of DNS servers and returning DNSSEC-signed zone transfer

In this figure, a zone is hosted on a pool of authoritative DNS servers. The servers are not secured with DNSSEC. The BIG-IP® system is configured with both a DNS zone and a DNSSEC zone that match the zone name on the servers. The BIG-IP system can forward zone transfer requests to a pool member, and then sign the response with DNSSEC keys, before sending the DNSSEC-signed zone transfer to the client (authoritative DNS nameserver or cloud provider). This allows the clients and cloud providers to serve DNSSEC-signed DNS queries and responses.

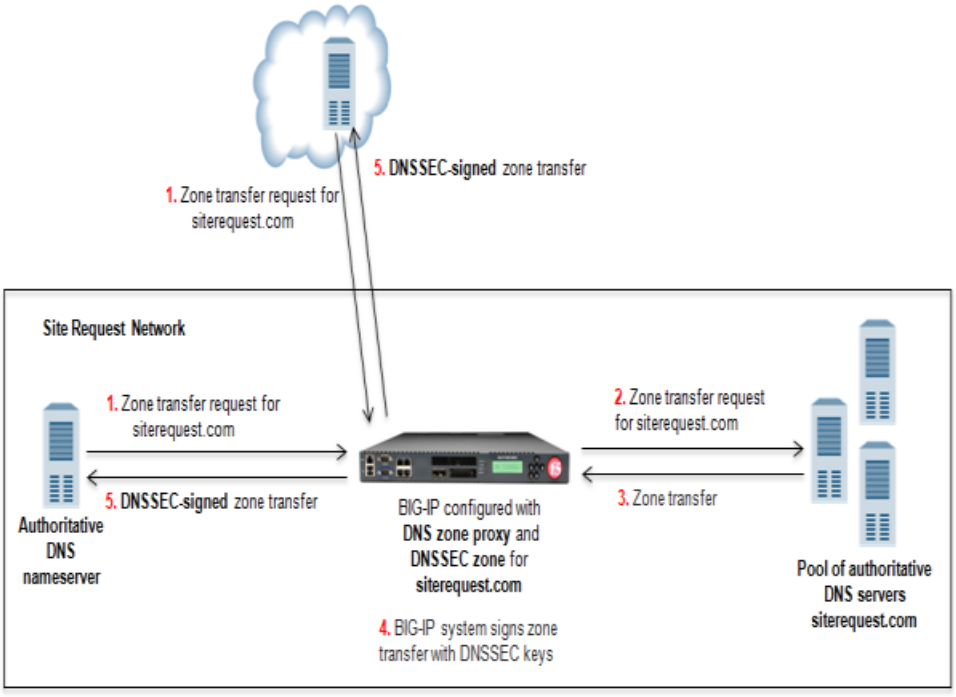


Figure 13: BIG-IP load balancing zone transfer request to pool member and returning DNSSEC-signed zone transfer

1. DNS nameserver (client) or cloud provider sends zone transfer request for a DNS zone.
2. BIG-IP forwards the request to a member of the pool of authoritative DNS servers that host the zone.
3. The pool member responds with a zone transfer.
4. BIG-IP signs the zone transfer with DNSSEC keys.
5. BIG-IP sends the DNSSEC-signed zone transfer to the client that made the request.

Important: *The DNSSEC feature is available only when the BIG-IP system is licensed for BIG-IP Global Traffic Manager™ (GTM™).*

Task summary

To configure the BIG-IP® system to sign zone transfers using DNSSEC keys, perform these tasks:

Enabling BIG-IP to respond to zone transfer requests
Enabling a DNS listener to process DNSSEC traffic
Creating automatically managed DNSSEC zone-signing keys
Creating manually managed DNSSEC zone-signing keys
Creating automatically managed DNSSEC key-signing keys
Creating manually managed DNSSEC key-signing keys
Creating a DNSSEC zone
Adding namserver objects that represent DNS servers
Adding nameserver objects that represent DNS nameservers (clients)
Configuring a DNS zone to answer zone transfer requests
Viewing DNSSEC zone statistics

Enabling BIG-IP to respond to zone transfer requests

To enable the BIG-IP® system to sign zone transfers, create a custom DNS profile, and then assign the profile to a listener.

1. On the Main tab, click **DNS** > **Delivery** > **Profiles** > **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. From the **Zone Transfer** list, select **Enabled**.
6. From the **Use BIND Server on BIG-IP** list, select **Disabled**.
7. Click **Finished**.

Assign the profile to a listener.

Important: *DNS zone transfers use TCP port 53. Ensure that you use at least one listener configured for TCP.*

Enabling a DNS listener to process DNSSEC traffic

Ensure that a custom DNS profile is present in the configuration with **Zone Transfer** enabled and **Use BIND server on BIG-IP** disabled.

When you implement DNSSEC zone transfer signing, you must modify the listeners that identify the DNSSEC traffic that the BIG-IP system handles by adding a custom DNS profile enabled for DNSSEC and zone transfers. If you created four listeners to handle your IPv4 and IPv6, UDP and TCP traffic, add the custom DNS profile to all four listeners.

Important: *DNS zone transfers use TCP port 53. Ensure that you use at least one listener configured for TCP.*

Note: *If you have multiple GTM systems in a device group, perform this procedure on only one GTM system.*

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 the custom DNS profile with **Zone Transfer** enabled, and **Use BIND server on BIG-IP** disabled.
4. Click **Finished**.
5. Perform steps 2 - 4 to modify each of the other listeners.

Creating automatically managed DNSSEC zone-signing keys

Ensure that the time setting on BIG-IP® GTM™ is synchronized with the NTP servers on your network. This ensures that each GTM in a synchronization group is referencing the same time when generating keys.

Determine the values you want to configure for the rollover period, expiration period, and TTL of the keys, using the following criteria:

- The amount of time required to send the DS records for the zone to which this key is associated to the organization that manages the parent zone.
- The value of the rollover period must be greater than half the value of the expiration period, as well as less than the value of the expiration period.
- The difference between the values of the rollover and expiration periods must be more than the value of the TTL.

Note: *The values recommended in this procedure are based on the values in the NIST Secure Domain Name System (DNS) Deployment Guide.*

Create automatically-managed zone-signing keys for GTM to use in the DNSSEC authentication process.

1. On the Main tab, click **DNS** > **Delivery** > **Keys** > **DNSSEC Key List**.
   The DNSSEC Key List screen opens.
2. Click **Create**.
   The New DNSSEC Key screen opens.
3. In the **Name** field, type a name for the key.

   Zone names are limited to `63` characters.
4. From the **Type** list, select **Zone Signing Key**.
5. From the **State** list, select **Enabled**.
6. From the **Hardware Security Module** list, select **None**.
7. From the **Algorithm** list, select the digest algorithm the system uses to generate the key signature. Your options are **RSA/SHA1**, **RSA/SHA256**, and **RSA/SHA512**.
8. From the **Key Management** list, select **Automatic**.
   The Key Settings area displays fields for key configuration.
9. In the **Bit Width** field, type `1024`.
10. In the **TTL** field, accept the default value of `86400` (the number of seconds in one day.)

    This value specifies how long a client resolver can cache the key. This value must be less than the difference between the values of the rollover and expiration periods of the key; otherwise, a client can make a query and the system can send a valid key that the client cannot recognize.
11. For the Rollover Period setting, in the **Days** field, type `21`.
12. For the Expiration Period setting, in the **Days** field, type `30`.

    Zero seconds indicates not set, and thus the key does not expire.
13. For the Signature Validity Period setting, accept the default value of seven days.

    This value must be greater than the value of the signature publication period.

    Zero seconds indicates not set, and thus the server verifying the signature never succeeds, because the signature is always expired.
14. For the Signature Publication Period setting, accept the default value of four days and 16 hours.

    This value must be less than the value of the signature validity period.

    Zero seconds indicates not set, and thus the signature is not cached.

15. Click **Finished**.
16. To create a standby key for emergency rollover purposes, repeat these steps using a similar name, and select **Disabled** from the **State** list.

Creating manually managed DNSSEC zone-signing keys

Ensure that the time setting on BIG-IP® GTM™ is synchronized with the NTP servers on your network. This ensures that each GTM in a synchronization group is referencing the same time when generating keys.

When you plan to manually create keys, install the certificate and key pairs on the BIG-IP system, before you attempt to create DNSSEC keys.

Important: *Certificate and key file pairs must have the same name, for example,* `exthsm.crt` *and* `exthsm.key`*.*

Create manually-managed zone-signing keys for GTM to use in the DNSSEC authentication process.

1. On the Main tab, click **DNS** > **Delivery** > **Keys** > **DNSSEC Key List**.
   The DNSSEC Key List screen opens.
2. Click **Create**.
   The New DNSSEC Key screen opens.
3. In the **Name** field, type a name for the key.
   Zone names are limited to `63` characters.
4. From the **Type** list, select **Zone Signing Key**.
5. From the **State** list, select **Enabled**.
6. From the **Hardware Security Module** list, select **None**.
7. From the **Algorithm** list, select the digest algorithm the system uses to generate the key signature. Your options are **RSA/SHA1**, **RSA/SHA256**, and **RSA/SHA512**.
8. From the **Key Management** list, select **Manual**.
   The Key Settings area displays **Certificate** and **Private Key** lists.
9. In the Key Settings area, select a certificate/key pair:
   a) From the **Certificate** list, select a certificate.
   b) From the **Private Key** list, select the key that matches the certificate you selected.
10. Click **Finished**.
11. To create a standby key for emergency rollover purposes, repeat these steps using a similar name, and select **Disabled** from the **State** list.

Creating automatically managed DNSSEC key-signing keys

Ensure that the time setting on BIG-IP® GTM™ is synchronized with the NTP servers on your network. This ensures that each GTM in a synchronization group is referencing the same time when generating keys.

Determine the values you want to configure for the rollover period, expiration period, and TTL of the keys, using the following criteria:

- The amount of time required to send the DS records for the zone to which this key is associated to the organization that manages the parent zone.

- The value of the rollover period must be greater than half the value of the expiration period, as well as less than the value of the expiration period.
- The difference between the values of the rollover and expiration periods must be more than the value of the TTL.

Note: *The values recommended in these steps are based on the values in the NIST Secure Domain Name System (DNS) Deployment Guide.*

Create key-signing keys for GTM to use in the DNSSEC authentication process.

1. On the Main tab, click **DNS** > **Delivery** > **Keys** > **DNSSEC Key List**.
   The DNSSEC Key List screen opens.
2. Click **Create**.
   The New DNSSEC Key screen opens.
3. In the **Name** field, type a name for the key.

   Zone names are limited to `63` characters.
4. From the **Type** list, select **Key Signing Key**.
5. From the **State** list, select **Enabled**.
6. From the **Hardware Security Module** list, select **None**.
7. From the **Algorithm** list, select the digest algorithm the system uses to generate the key signature. Your options are **RSA/SHA1**, **RSA/SHA256**, and **RSA/SHA512**.
8. From the **Key Management** list, select **Automatic**.
   The Key Settings area displays fields for key configuration.
9. In the **Bit Width** field, type `2048`.
10. In the **TTL** field, accept the default value of `86400` (the number of seconds in one day.)

    This value specifies how long a client resolver can cache the key. This value must be less than the difference between the values of the rollover and expiration periods of the key; otherwise, a client can make a query and the system can send a valid key that the client cannot recognize.
11. For the Rollover Period setting, in the **Days** field, type `340`.
12. For the Expiration Period setting, in the **Days** field, type `365`.

    Zero seconds indicates not set, and thus the key does not expire.

    Tip: *The National Institute of Standards and Technology (NIST) recommends that a key-signing key expire once a year.*

    ---
13. For the Signature Validity Period setting, accept the default value of seven days.

    This value must be greater than the value of the signature publication period.

    Zero seconds indicates not set, and thus the server verifying the signature never succeeds, because the signature is always expired.
14. For the Signature Publication Period setting, accept the default value of four days and 16 hours.

    This value must be less than the value of the signature validity period.

    Zero seconds indicates not set, and thus the signature is not cached.
15. Click **Finished**.
16. To create a standby key for emergency rollover purposes, repeat these steps using a similar name, and select **Disabled** from the **State** list.

Creating manually managed DNSSEC key-signing keys

Ensure that the time setting on BIG-IP® GTM™ is synchronized with the NTP servers on your network. This ensures that each GTM in a synchronization group is referencing the same time when generating keys.

When you plan to manually create keys, install the certificate and key pairs on the BIG-IP system, before you attempt to create DNSSEC keys.

Important: *Certificate and key file pairs must have the same name, for example,* `exthsm.crt` *and* `exthsm.key`*.*

Create key-signing keys for GTM to use in the DNSSEC authentication process.

1. On the Main tab, click **DNS** > **Delivery** > **Keys** > **DNSSEC Key List**.
   The DNSSEC Key List screen opens.
2. Click **Create**.
   The New DNSSEC Key screen opens.
3. In the **Name** field, type a name for the key.
   Zone names are limited to `63` characters.
4. From the **Type** list, select **Key Signing Key**.
5. From the **State** list, select **Enabled**.
6. From the **Hardware Security Module** list, select **None**.
7. From the **Algorithm** list, select the digest algorithm the system uses to generate the key signature. Your options are **RSA/SHA1**, **RSA/SHA256**, and **RSA/SHA512**.
8. From the **Key Management** list, select **Manual**.
   The Key Settings area displays **Certificate** and **Private Key** lists.
9. In the Key Settings area, select a certificate/key pair:
   a) From the **Certificate** list, select a certificate.
   b) From the **Private Key** list, select the key that matches the certificate you selected.
10. Click **Finished**.
11. To create a standby key for emergency rollover purposes, repeat these steps using a similar name, and select **Disabled** from the **State** list.

Creating a DNSSEC zone

Before you configure DNSSEC, ensure that at least one data center and a server object representing the BIG-IP® device exist in the BIG-IP system configuration.

Important: *The DNSSEC feature is available only when the BIG-IP system is licensed for BIG-IP Global Traffic Manager™ (GTM™).*

Before the BIG-IP system can sign DNS requests (including zone transfer requests) for a zone using DNSSEC keys, you must create a DNSSEC zone on the system and assign at least one enabled zone-signing and one enabled key-signing key to the zone.

1. On the Main tab, click **DNS** > **Zones** > **DNSSEC Zones**.
   The DNSSEC Zone List screen opens.
2. Click **Create**.

The New DNSSEC Zone screen opens.

3. In the **Name** field, type a domain name.
   For example, use a zone name of `siterequest.com` to handle DNSSEC requests for `www.siterequest.com` and `*.www.sitrequest.com`.
4. From the **State** list, select **Enabled**.
5. For the **Zone Signing Key** setting, assign at least one enabled zone-signing key to the zone.
   You can associate the same zone-signing key with multiple zones.
6. For the **Key Signing Key** setting, assign at least one enabled key-signing key to the zone.
   You can associate the same key-signing key with multiple zones.
7. Click **Finished**.
   Even if you selected **Enabled** from the **State** list, if there are not at least one zone-signing and one key-signing key in the Active column, the status of the zone changes to offline.

Upload the DS records for this zone to the organization that manages the parent zone. The administrators of the parent zone sign the DS record with their own key and upload it to their zone. You can find the DS records in the Configuration utility.

Adding namserver objects that represent DNS servers

Obtain the IP address of the authoritative DNS server that hosts the DNS zone. Optional: Ensure that the server TSIG key is available on the BIG-IP system.

When you want to transfer a zone from an authoritative DNS server into the DNS Express™ engine and have DNS Express respond to DNS queries for the zone, add a nameserver object that represents the server that hosts the zone.

1. On the Main tab, click **DNS** > **Delivery** > **Nameservers**.
   The Nameservers List screen opens.
2. Click **Create**.
   The New Nameserver screen opens.
3. In the **Name** field, type a name for the authoritative DNS server.
4. In the **Address** field, type the IP address on which the DNS server listens for DNS messages.
5. Optional: From the **Server Key** list, select the TSIG key that matches the TSIG key on the DNS server.
   The BIG-IP system uses this TSIG key to sign DNS zone transfer requests sent to the DNS server that hosts this zone, and then to verify a zone transfer returned from the DNS server.

Create a DNS zone and add a DNS Express server object to the zone.

Adding nameserver objects that represent DNS nameservers (clients)

Gather the IP addresses of the DNS nameservers (clients) from which the DNS Express™ engine accepts zone transfer requests for a DNS zone. Optional: Ensure that the client TSIG key is available on the BIG-IP system.

To allow DNS nameservers (clients) to request zone transfers for a zone, add a nameserver object that represents each client. Optionally, you can add a client TSIG key that the BIG-IP system uses to authenticate the identity of the client during zone transfer communications.

1. On the Main tab, click **DNS** > **Delivery** > **Nameservers**.

The Nameservers List screen opens.

2. Click **Create**.
   The New Nameserver screen opens.
3. In the **Name** field, type a name for the DNS nameserver (client).
4. In the **Address** field, type the IP address on which the DNS nameserver (client) listens for DNS messages.
5. Optional: If you want the BIG-IP system to validate a zone transfer request from this client, from the **TSIG Key** list, select the client TSIG key.

   If there is a TSIG key configured on this client, the BIG-IP system uses the key to validate a zone transfer request from this client, and adds a signature for this key to a zone transfer response sent from a DNS server, a pool member, or DNS Express.
6. Click **Finished**.
7. Add nameserver objects to represent other DNS nameservers (clients).

Add the DNS nameservers (clients) objects to the **Zone Transfer Client** list of the DNS zone on the BIG-IP system.

Configuring a DNS zone to answer zone transfer requests

Ensure that at least one nameserver object that represents a DNS nameserver (client) exists in the BIG-IP® system configuration:

Modify a DNS zone to answer zone transfer requests from specific DNS nameservers (clients).

1. On the Main tab, click **DNS** > **Zones**.
   The Zone List screen opens.
2. Click the name of the zone you want to modify.
3. In the Zone Transfer Clients area, move the nameservers that can initiate zone transfers from the **Available** list to the **Active** list.
4. Click **Finished**.

Viewing DNSSEC zone statistics

You can view information about the zones that are protected by DNS Express™.

1. On the Main tab, click **Statistics** > **Module Statistics** > **DNS** > **Zones**.
   The Zones statistics screen opens.
2. From the **Statistics Type** list, select **DNSSEC Zones**.
   Information displays about the traffic handled by the DNSSEC zones in the list.
3. In the Details column for a zone, click **View**.
   Read the online help for an explanation of the statistics.

Troubleshooting DNSSEC on the BIG-IP system

On BIG-IP® GTM™, you can view DNSSEC records in ZoneRunner™, access and view DNSSEC SEP Records, and modify generations of a DNSSEC key.

Task summary

When you want to troubleshoot the DNSSEC configuration on GTM, perform these tasks.

Viewing DNSSEC records in ZoneRunner

Accessing DNSSEC SEP records

Modifying generations of a DNSSEC key

Viewing DNSSEC records in ZoneRunner

Ensure that all DNSSEC records are added to the BIND configuration.

View the DNSSEC records using ZoneRunner™ when you want to evaluate how your network is handling DNSSEC traffic.

1. On the Main tab, click **DNS** > **Zones** > **ZoneRunner** > **Resource Record List**.
   The Resource Record List screen opens.
2. From the **View Name** list, select the name of the view that contains the resource records you want to view.
3. From the **Zone Name** list, select the zone for which you want to view resource records.
4. From the **Type** list, select the type of resource records you want to view.
5. Click **Search**.

View the resource records that display.

Accessing DNSSEC SEP records

Ensure that the BIG-IP system contains at least one DNSSEC zone.

Access the SEP records associated with a DNSSEC zone, when you want to copy the DS or DNSKEY records for the zone.

1. On the Main tab, click **DNS** > **Zones** > **DNSSEC Zones**.
   The DNSSEC Zone List screen opens.
2. Click the name of the DNSSEC zone for which you want to view or copy SEP records.
3. On the menu bar, click **SEP Records**.
   The SEP records display for each generation of a key. If the SEP record screen is unexpectedly blank, ensure that at least one data center and a server representing the BIG-IP GTM device exist in the BIG-IP system configuration.
4. From the **Generation** list, select a generation of the key-signing key.
   The **DS Record** and **DNSKEY Record** fields display read-only Security Entry Point (SEP) records, specifically the DS (Delegation Signer) and DNSKey records.

Modifying generations of a DNSSEC key

Modify a generation of a DNSSEC key, when you want to perform an emergency rollover of a compromised key for which you do not have a standby key.

1. On the Main tab, click **DNS** > **Delivery** > **Keys** > **DNSSEC Key List**.
   The DNSSEC Key List screen opens.
2. Click a number in the Generations column.

Information about this generation of the key displays.

Column Title	Contains
ID	Generation number of the key
Key Tag	Identifier (hash) of this generation of the key
Creator	Host name of BIG-IP GTM that created this generation of the key
Rollover Time	Time this generation of the key will roll over
Expiration Time	Time this generation of the key will expire

3. Click the number in the ID column.
   The general properties of the generation of the key display.
4. Select **Specify** from the **Rollover Time** list, and then select the exact time that you want the BIG-IP system to create and begin to use a new generation of this key.

   Modifying this setting does not affect the value of the rollover and expiration periods of the key.
5. Select **Specify** from the **Expiration Time** list, and then select the exact time that you want this generation of the key to expire.

   Modifying this setting does not affect the value of the rollover and expiration periods of the key.
6. Click **Update**.

Chapter 5

Configuring DNS Caching

Overview: Using caching to improve DNS performance

You can configure a DNS cache on the BIG-IP® system to allow the system to more quickly respond to repeated DNS queries. You can configure a simple DNS cache or a DNS cache with more advanced resolving and validation functions. There are three types of DNS cache configurations available on the BIG-IP system: a transparent cache, a resolver cache, and a validating resolver cache.

Typically, you configure a resolver cache where the BIG-IP system either acts as the LDNS for clients or is in the LDNS resolver path for clients. By caching DNS responses and answering queries from the cache, the BIG-IP system is able to immediately respond to subsequent client requests for the same resource. This enhances DNS performance in two significant ways. First, answering a DNS query from the cache is faster and has a very short latency, because the sooner a client gets a DNS response, the faster the client can access the Internet resource. Secondly, caching DNS responses reduces the number of queries that have to be resolved. The BIG-IP system uses the cache to resolve the same query from multiple clients handling many more queries per second than a typical DNS resolver.

About the transparent DNS cache

You can configure a transparent cache on the BIG-IP® system to use external DNS resolvers to resolve queries, and then cache the responses from the resolvers. The next time the system receives a query for a response that exists in the cache, the system immediately returns the response from the cache. The transparent cache contains messages and resource records.

A *transparent cache* in the BIG-IP system consolidates content that would otherwise be cached across multiple external resolvers. When a consolidated cache is in front of external resolvers (each with their own cache), it can produce a much higher cache hit percentage.

F5 Networks recommends that you configure the BIG-IP system to forward queries, which cannot be answered from the cache, to a pool of local DNS servers rather than the local BIND instance because BIND performance is slower than using multiple external resolvers.

Note: *For systems using the DNS Express™ feature, the BIG-IP system first processes the requests through DNS Express, and then caches the responses.*

About the resolver DNS cache

You can configure a resolver cache on the BIG-IP® system to resolve DNS queries and cache the responses. The next time the system receives a query for a response that exists in the cache, the system returns the response from the cache. The *resolver cache* contains messages, resource records, and the nameservers the system queries to resolve DNS queries.

It is important for network architects to note that it is possible to configure the local BIND instance on the BIG-IP® system to act as an external DNS resolver. However, F5 Networks does not recommend this approach, because the performance of BIND is slower than using a resolver cache.

About the validating resolver DNS cache

You can configure a validating resolver cache on the BIG-IP® system to recursively query public DNS servers, validate the identity of the DNS server sending the responses, and then cache the responses. The

next time the system receives a query for a response that exists in the cache, the system returns the DNSSEC-compliant response from the cache. The *validating resolver* cache contains messages, resource records, the nameservers the system queries to resolve DNS queries, and DNSSEC keys.

Using the validating resolver cache, the BIG-IP system mitigates cache poisoning by validating DNS responses using DNSSEC validation. This is important, because attackers can attempt to populate a DNS cache with erroneous data that redirects clients to fake web sites, or downloads malware and viruses to client computers. When an authoritative server signs a DNS response, the validating resolver verifies the data before entering the data into the cache. Additionally, the validating resolver cache includes a built-in filter and detection mechanism that rejects unsolicited DNS responses.

About information stored in DNS caches

The transparent, resolver, and validating resolver DNS caches contain a message cache and a resource record cache. The resolver and validating resolver DNS caches also contain a nameserver cache. Additionally, the validating resolver cache contains a key cache.

Message cache

The message cache contains the entire contents of a particular DNS response including the supporting records.

Resource Record cache

The resource record cache contains the individual record elements in the DNS response, which may include an SOA record, DNSSEC key records, glue records, and other supporting records.

Nameserver cache

The nameserver cache contains information about the public DNS nameservers the resolver has used to fill the cache. Often there is more than one nameserver that is listed as an authority for a zone; therefore, the cache entries track metrics for the nameservers so that the system can send new queries to the best nameserver. The cache entries include metrics, such as time to live (TTL), round trip times (RRT), and properties, such as EDNS support and zone lameness.

Key cache

The key cache contains the DNSKEY resource records and tracks the DNSSEC keys for use in DNSSEC validation. This cache also contains information about the validity of the DNSSEC keys.

Configuring DNS cache global settings

Configure the global settings on the BIG-IP® system to specify how the system manages the DNS caches you create.

1. On the Main tab, click **DNS** > **Settings** > **Caches**.
   The DNS Cache configuration screen opens.
2. In the **Minimum TTL** field, type the minimum number of seconds you want the system to cache DNS resource records.

   Note: *When you configure this setting the system can cache resource records longer than the owner of the records intended.*

3. In the **Maximum TTL** field, type the number of seconds after which you want the system to re-query for resource records.

Warning: *With this setting, the system can re-query for resource records sooner than the owner of the records intended.*

4. In the **EDNS Buffer Size** field, type the number of bytes you want the system to advertise as the EDNS buffer size in UDP queries.

   The default value of **4096** bytes is the default value for ENDS0.

5. Click **Update**.

After you configure the DNS global settings, create at least one DNS cache.

Overview: Caching responses from external resolvers

You can configure a transparent cache on the BIG-IP® system to use external DNS resolvers to resolve queries, and then cache the responses from the resolvers. The next time the BIG-IP system receives a query for a response that exists in the cache, the system immediately returns the response from the cache. The transparent cache contains messages and resource records.

A *transparent cache* in the BIG-IP system consolidates content that would otherwise be cached across multiple external resolvers. When a consolidated cache is in front of external resolvers (each with their own cache), it can produce a much higher cache hit percentage.

Tip: *F5® Networks recommends that you configure the BIG-IP system to forward queries, which cannot be answered from the cache, to a pool of local DNS servers rather than the local BIND instance because BIND performance is slower than using multiple external resolvers.*

Note: *For systems using the DNS Express™ feature, the BIG-IP system first processes the requests through DNS Express, and then caches the responses.*

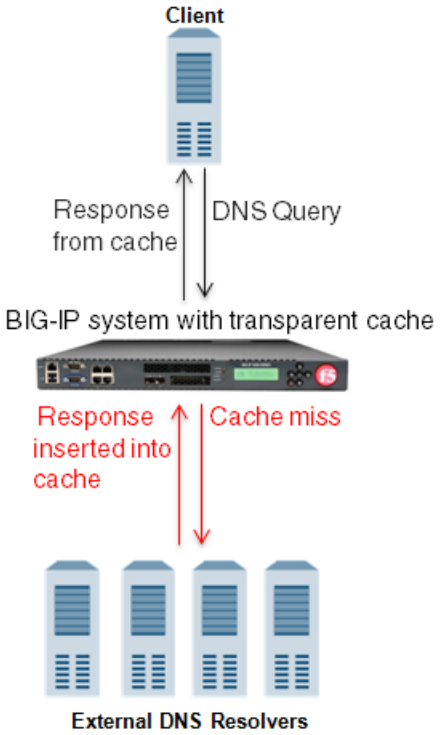


Figure 14: BIG-IP system using transparent cache

Task summary

Creating a transparent DNS cache
Enabling transparent DNS caching
Assigning a custom DNS profile to an LTM virtual server
Assigning a custom DNS caching profile to a GTM listener
Creating a custom DNS monitor
Creating a pool of local DNS servers
Determining DNS cache performance
Clearing a DNS cache

Creating a transparent DNS cache

Create a transparent cache on the BIG-IP® system when you want the system to cache DNS responses from external DNS resolvers.

1. On the Main tab, click **DNS** > **Caches** > **Cache List**.
   The DNS Cache List screen opens.
2. Click **Create**.
   The New DNS Cache screen opens.
3. In the **Name** field, type a name for the cache.
4. From the **Resolver Type** list, select **Transparent**.
5. Click **Finished**.

Associate the DNS cache with a custom DNS profile.

Enabling transparent DNS caching

Ensure that at least one transparent cache exists on the BIG-IP® system.

To enable the BIG-IP system to cache responses to DNS queries, create a custom DNS profile and associate it with a transparent DNS cache.

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. In the **Parent Profile** list, accept the default **dns** profile.
5. Select the **Custom** check box.
6. From the **Use BIND Server on BIG-IP** list, select **Disabled**.
7. From the **DNS Cache** list, select **Enabled**.
   When you enable the **DNS Cache** option, you must also select a DNS cache from the **DNS Cache Name** list.
8. From the **DNS Cache Name** list, select the DNS cache that you want to associate with this profile.
   You can associate a DNS cache with a profile, even when the **DNS Cache** option, is **Disabled**.
9. Click **Finished**.

Assign the custom DNS profile to the virtual server or listener that handles the DNS traffic from which you want to cache responses.

Assigning a custom DNS profile to an LTM virtual server

Ensure that at least one custom DNS profile that is configured for DNS caching exists on the BIG-IP® system.

Assign a custom DNS profile to a virtual server when you want the BIG-IP system to perform DNS caching on traffic that 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 the custom DNS profile you created.
5. Click **Update** to save the changes.

The responses to DNS queries handled by this virtual server are cached on the BIG-IP system.

Assigning a custom DNS caching profile to a GTM listener

Ensure that at least one custom DNS profile that is configured for DNS caching exists on the BIG-IP® system.

Assign a custom DNS profile to a listener when you want the BIG-IP system to perform DNS caching on traffic that 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 configured for DNS caching.
4. Click **Update**.

Creating a custom DNS monitor

Create a custom DNS monitor to send DNS queries, generated using the settings you specify, to a pool of DNS servers and validate the DNS responses.

Important: *When defining values for custom monitors, make sure you avoid using any values that are on the list of reserved keywords. For more information, see SOL 3653 (for version 9.0 systems and later) on the AskF5™ technical support web site at* `www.askf5.com`.

---

1. On the Main tab, click **DNS** > **Delivery** > **Load Balancing** > **Monitors** or **Local Traffic** > **Monitors**.
   The Monitor List screen opens.
2. Click **Create**.
   The New Monitor screen opens.
3. Type a name for the monitor in the **Name** field.
4. From the **Type** list, select **DNS**.
5. In the **Query Name** field, type the domain name that you want the monitor to query.
   For the zone, `siterequest.com`, you might want the monitor to query for `www.siterequest.com`.
6. Configure additional settings based on your network requirements.
7. Click **Finished**.

Creating a pool of local DNS servers

Ensure that at least one custom DNS monitor exists on the BIG-IP® system. Gather the IP addresses of the DNS servers that you want to include in a pool to which the BIG-IP system load balances DNS traffic.

Create a pool of local DNS servers when you want to load balance DNS queries to other DNS servers.

1. On the Main tab, click **DNS** > **Delivery** > **Load Balancing** > **Pools** or **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 custom DNS monitor you created, and click **<<** to move the monitor to the **Active** list.
5. Using the **New Members** setting, add each resource that you want to include in the pool:
   a) Type an IP address in the **Address** field.
   b) Type a port number in the **Service Port** field, or select a service name from the list.
   c) To specify a priority group, type a priority number in the **Priority Group Activation** field.
   d) Click **Add**.
6. Click **Finished**.

Determining DNS cache performance

Ensure that you have created a DNS cache and associated it with a DNS profile, and have assigned the profile to either an LTM® virtual server or a GTM™ listener.

You can view statistics to determine how well a DNS cache on the BIG-IP® system is performing.

1. On the Main tab, click **Statistics** > **Module Statistics** > **DNS** > **Caches**.
   The DNS Caches Status Summary screen opens.
2. From the **Statistics Type** list, select **Caches**.
   Information displays about the DNS caches.

Record type	Description
Queries	Total number of queries handled by the cache.
Responses	Total number of responses sent from the cache.
Sync	Number of synchronous queries handled by the cache.
Async	Number of asynchronous queries handled by the cache.
Resolve	Total number of DNS resolve failures.
Connect	Total number of DNS connect failures.
Server	Number of DNS server failures.
Send	Number of DNS response send failures.

3. In the Details column for a cache, click **View** to display detailed information about the cache.
4. To return to the DNS Cache Statistics screen, click the **Back** button.

Viewing records in a DNS cache

You can view records in a DNS cache to determine how well a specific cache on the BIG-IP® system is performing.

1. Log in to the command-line interface of the BIG-IP system.
2. At the BASH prompt, type the command:

```
tmsh
```

3. At the `tmsh` prompt, type the command:

   ```
   show ltm dns cache records rrset cache <cache name>
   ```

   For example, the command: `show ltm dns cache records rrset cache my_transparent_cache`, displays the resource records in the cache named *my_transparent_cache*.

Viewing DNS cache statistics in the Configuration utility

Ensure that you have created a DNS cache and a DNS profile and have assigned the profile to either an LTM® virtual server or a GTM™ listener.

You can view DNS cache statistics to determine how well a specific cache on the BIG-IP® system is performing.

1. On the Main tab, click **Statistics** > **Module Statistics** > **DNS** > **Caches**.
   The DNS Caches Status Summary screen opens.
2. From the **Statistics Type** list, select **Caches**.
3. In the Details column for a cache, click **View** to display detailed information about the cache.
4. To return to the DNS Cache Statistics screen, click the **Back** button.

Viewing DNS cache statistics using tmsh

You can view DNS cache statistics to determine how well a specific cache on the BIG-IP® system is performing.

1. On the Main tab, click **Statistics** > **Module Statistics** > **DNS** > **Caches**.
   The DNS Caches Status Summary screen opens.
2. From the **Statistics Type** list, select **Caches**.
   Information displays about the DNS caches.

Record type	Description
Queries	Total number of queries handled by the cache.
Responses	Total number of responses sent from the cache.
Sync	Number of synchronous queries handled by the cache.
Async	Number of asynchronous queries handled by the cache.
Resolve	Total number of DNS resolve failures.
Connect	Total number of DNS connect failures.
Server	Number of DNS server failures.
Send	Number of DNS response send failures.

3. To return to the DNS Cache Statistics screen, click the **Back** button.

Managing transparent cache size

Determine the amount of memory the BIG-IP® system has and how much of that memory you want to commit to DNS caching. View the statistics for a cache to determine how well the cache is working.

You can change the size of a DNS cache to fix cache performance issues.

1. On the Main tab, click **DNS** > **Caches** > **Cache List**.
   The DNS Cache List screen opens.
2. Click the name of the cache you want to modify.
   The properties screen opens.
3. In the **Message Cache Size** field, type the maximum size in bytes for the DNS message cache.

   The BIG-IP system caches the messages in a DNS response in the message cache. A higher maximum size makes it possible for more DNS responses to be cached and increases the cache hit percentage. A lower maximum size forces earlier eviction of cached content, but can lower the cache hit percentage.

   Important: *When you change the value of the* ***Message Cache Size****, the records in the message cache are automatically removed. If you do not want to clear the message cache, do not change the value of this parameter.*
4. In the **Resource Record Cache Size** field, type the maximum size in bytes for the DNS resource record cache.

   The BIG-IP system caches the supporting records in a DNS response in the Resource Record cache. A higher maximum size makes it possible for more DNS responses to be cached and increases the cache hit percentage. A lower maximum size forces earlier eviction of cached content, but can lower the cache hit percentage. .

   Warning: *When you change the value of the* ***Resource Record Cache Size****, the records in the resource record cache are automatically removed from the cache. If you do not want to clear the resource record cache, do not change the value of this parameter.*
5. In the **Nameserver Cache Count** field, type the maximum number of DNS nameservers for which the BIG-IP® system caches connection and capability data.

   Important: *When you change the value of the* ***Nameserver Cache Count****, the records in the nameserver cache are automatically removed from the cache. If you do not want to clear the nameserver cache, do not change the value of this parameter.*
6. Click **Finished**.

Clearing a DNS cache

You can clear all records from a specific DNS cache on the BIG-IP® system.

1. On the Main tab, click **DNS** > **Caches** > **Cache List**.
   The DNS Cache List screen opens.
2. On the menu bar, click **Statistics**.
   The Local Traffic Statistics screen opens.
3. Select the check box next to the cache you want to clear, and then click **Clear Cache**.

Clearing groups of records from a DNS cache

You can clear groups of records of a specific type from a DNS cache by resizing the cache that contains those records.

1. On the Main tab, click **DNS** > **Caches** > **Cache List**.
   The DNS Cache List screen opens.
2. Click the name of the cache you want to modify.
   The properties screen opens.
3. In the DNS Cache area, to clear specific records from the cache, do one of the following:

Option	Description
To clear messages from the cache:	change the value in the **Message Cache Size** field.
To clear resource records from the cache:	change the value in the **Resource Record Cache Size** field.
To clear nameservers from the cache:	change the value in the **Name Server Cache Count** field.
To clear DNSSEC keys from the cache:	change the value in the **DNSSEC Key Cache Size** field.

4. Click **Update**.

The BIG-IP® system clears the records in the caches that you resized.

Clearing specific records from a DNS cache using tmsh

You can clear specific records from a DNS cache using `tmsh`. For example, you can delete all RRSET records or only the A records in the specified cache.

Tip: *In `tmsh`, you can use the command completion feature to discover the types of records that are available for deletion.*

1. Log in to the command-line interface of the BIG-IP® system.
2. At the BASH prompt, type the command:
   ```
   tmsh
   ```
3. At the `tmsh` prompt, to navigate to the directory that contains the DNS cache records, type the command:
   ```
   ltm dns cache records
   ```
4. To delete specific DNS cache records, type a variation of this command:
   ```
   delete <cache-type> type <record-type> cache <cache-name>
   ```
   For example, the command `delete rrset type a cache my_resolver_cache`, deletes the A records from the resource record cache of the resolver cache named *`my_resolver_cache`*.

Overview: Resolving queries and caching responses

You can configure the BIG-IP® system to resolve DNS queries and cache the responses by creating a resolver DNS cache. The next time the BIG-IP system receives a query for a response that exists in the cache, the

system returns the response from the cache. The *resolver cache* contains messages, resource records, and the nameservers the system queries to resolve DNS queries.

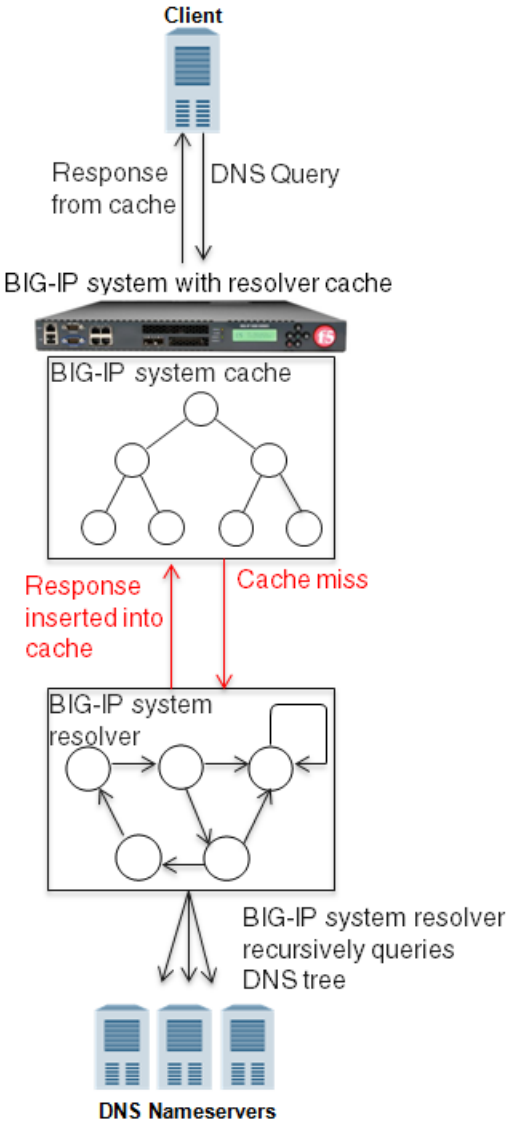


Figure 15: BIG-IP system using resolver cache

Task summary

Creating a resolver DNS cache
Enabling resolving and caching
Determining DNS cache performance
Clearing a DNS cache

Creating a resolver DNS cache

Create a resolver cache on the BIG-IP® system when you want the system to resolve DNS queries and cache responses.

1. On the Main tab, click **DNS** > **Caches** > **Cache List**.
   The DNS Cache List screen opens.

2. Click **Create**.
   The New DNS Cache screen opens.
3. In the **Name** field, type a name for the cache.
4. From the **Resolver Type** list, select **Resolver**.
5. Click **Finished**.

Associate the DNS cache with a custom DNS profile.

Enabling resolving and caching

Ensure that at least one DNS cache exists on the BIG-IP® system.

To enable the BIG-IP system to resolve DNS queries and cache the responses, create a custom DNS profile and associate it with a resolver DNS cache.

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. From the **Use BIND Server on BIG-IP** list, select **Disabled**.
6. From the **DNS Cache** list, select **Enabled**.
   When you enable the **DNS Cache** option, you must also select a DNS cache from the **DNS Cache Name** list.
7. From the **DNS Cache Name** list, select the DNS cache that you want to associate with this profile.
   You can associate a DNS cache with a profile, even when the **DNS Cache** option, is **Disabled**.
8. Click **Finished**.

Assign the custom DNS profile to the virtual server or listener that handles the DNS traffic.

Determining DNS cache performance

Ensure that you have created a DNS cache and associated it with a DNS profile, and have assigned the profile to either an LTM® virtual server or a GTM™ listener.

You can view statistics to determine how well a DNS cache on the BIG-IP® system is performing.

1. On the Main tab, click **Statistics** > **Module Statistics** > **DNS** > **Caches**.
   The DNS Caches Status Summary screen opens.
2. From the **Statistics Type** list, select **Caches**.
   Information displays about the DNS caches.

Record type	Description
Queries	Total number of queries handled by the cache.
Responses	Total number of responses sent from the cache.

Record type	Description
Sync	Number of synchronous queries handled by the cache.
Async	Number of asynchronous queries handled by the cache.
Resolve	Total number of DNS resolve failures.
Connect	Total number of DNS connect failures.
Server	Number of DNS server failures.
Send	Number of DNS response send failures.

3. In the Details column for a cache, click **View** to display detailed information about the cache.
4. To return to the DNS Cache Statistics screen, click the **Back** button.

Viewing records in a DNS cache

You can view records in a DNS cache to determine how well a specific cache on the BIG-IP® system is performing.

1. Log in to the command-line interface of the BIG-IP system.
2. At the BASH prompt, type the command:
   ```
   tmsh
   ```
3. At the `tmsh` prompt, type the command:
   ```
   show ltm dns cache records rrset cache <cache name>
   ```
   For example, the command: `show ltm dns cache records rrset cache my_transparent_cache`, displays the resource records in the cache named *my_transparent_cache*.

Viewing DNS cache statistics in the Configuration utility

Ensure that you have created a DNS cache and a DNS profile and have assigned the profile to either an LTM® virtual server or a GTM™ listener.

You can view DNS cache statistics to determine how well a specific cache on the BIG-IP® system is performing.

1. On the Main tab, click **Statistics** > **Module Statistics** > **DNS** > **Caches**.
   The DNS Caches Status Summary screen opens.
2. From the **Statistics Type** list, select **Caches**.
3. In the Details column for a cache, click **View** to display detailed information about the cache.
4. To return to the DNS Cache Statistics screen, click the **Back** button.

Viewing DNS cache statistics using tmsh

You can view DNS cache statistics to determine how well a specific cache on the BIG-IP® system is performing.

1. On the Main tab, click **Statistics** > **Module Statistics** > **DNS** > **Caches**.

The DNS Caches Status Summary screen opens.

2. From the **Statistics Type** list, select **Caches**.
   Information displays about the DNS caches.

Record type	Description
Queries	Total number of queries handled by the cache.
Responses	Total number of responses sent from the cache.
Sync	Number of synchronous queries handled by the cache.
Async	Number of asynchronous queries handled by the cache.
Resolve	Total number of DNS resolve failures.
Connect	Total number of DNS connect failures.
Server	Number of DNS server failures.
Send	Number of DNS response send failures.

3. To return to the DNS Cache Statistics screen, click the **Back** button.

Managing cache size

Determine the amount of memory the BIG-IP® system has and how much you want to commit to DNS caching. View the statistics for a cache to determine how well the cache is working.

You can change the size of a DNS cache to fix cache performance issues.

1. On the Main tab, click **DNS** > **Caches** > **Cache List**.
   The DNS Cache List screen opens.
2. Click the name of the cache you want to modify.
   The properties screen opens.
3. In the **Message Cache Size** field, type the maximum size in bytes for the DNS message cache.
   The BIG-IP system caches the messages in a DNS response in the message cache. A higher maximum size makes it possible for more DNS responses to be cached and increases the cache hit percentage. A lower maximum size forces earlier eviction of cached content, but can lower the cache hit percentage.

   Important: *When you change the value of the* ***Message Cache Size****, the records in the message cache are automatically removed. If you do not want to clear the message cache, do not change the value of this parameter.*

4. In the **Resource Record Cache Size** field, type the maximum size in bytes for the DNS resource record cache.
   The BIG-IP system caches the supporting records in a DNS response in the Resource Record cache. A higher maximum size makes it possible for more DNS responses to be cached and increases the cache hit percentage. A lower maximum size forces earlier eviction of cached content, but can lower the cache hit percentage. .

   Warning: *When you change the value of the* ***Resource Record Cache Size****, the records in the resource record cache are automatically removed from the cache. If you do not want to clear the resource record cache, do not change the value of this parameter.*

5. In the **Nameserver Cache Count** field, type the maximum number of DNS nameservers for which the BIG-IP® system caches connection and capability data.

   Important: *When you change the value of the* ***Nameserver Cache Count****, the records in the nameserver cache are automatically removed from the cache. If you do not want to clear the nameserver cache, do not change the value of this parameter.*

6. In the **Unsolicited Reply Threshold** field, change the default value if you are using the BIG-IP® system to monitor for unsolicited replies using SNMP.

   The system always rejects unsolicited replies. The default value of 0 (off) indicates the system does not generate SNMP traps or log messages when rejecting unsolicited replies. Changing the default value alerts you to a potential security attack, such as cache poisoning or DOS. For example, if you specify 1,000,000 unsolicited replies, each time the system receives 1,000,000 unsolicited replies, it generates an SNMP trap and log message.

7. Click **Update**.

Clearing a DNS cache

You can clear all records from a specific DNS cache on the BIG-IP® system.

1. On the Main tab, click **DNS** > **Caches** > **Cache List**.
   The DNS Cache List screen opens.
2. On the menu bar, click **Statistics**.
   The Local Traffic Statistics screen opens.
3. Select the check box next to the cache you want to clear, and then click **Clear Cache**.

Clearing groups of records from a DNS cache

You can clear groups of records of a specific type from a DNS cache by resizing the cache that contains those records.

1. On the Main tab, click **DNS** > **Caches** > **Cache List**.
   The DNS Cache List screen opens.
2. Click the name of the cache you want to modify.
   The properties screen opens.
3. In the DNS Cache area, to clear specific records from the cache, do one of the following:

Option	Description
To clear messages from the cache:	change the value in the **Message Cache Size** field.
To clear resource records from the cache:	change the value in the **Resource Record Cache Size** field.
To clear nameservers from the cache:	change the value in the **Name Server Cache Count** field.
To clear DNSSEC keys from the cache:	change the value in the **DNSSEC Key Cache Size** field.

4. Click **Update**.

The BIG-IP® system clears the records in the caches that you resized.

Clearing specific records from a DNS cache using tmsh

You can clear specific records from a DNS cache using `tmsh`. For example, you can delete all RRSET records or only the A records in the specified cache.

Tip: *In `tmsh`, you can use the command completion feature to discover the types of records that are available for deletion.*

1. Log in to the command-line interface of the BIG-IP® system.
2. At the BASH prompt, type the command:
   ```
   tmsh
   ```
3. At the `tmsh` prompt, to navigate to the directory that contains the DNS cache records, type the command:
   ```
   ltm dns cache records
   ```
4. To delete specific DNS cache records, type a variation of this command:
   ```
   delete <cache-type> type <record-type> cache <cache-name>
   ```
   For example, the command `delete rrset type a cache my_resolver_cache`, deletes the A records from the resource record cache of the resolver cache named *my_resolver_cache*.

Overview: Resolving queries and caching validated responses

You can configure the BIG-IP® system to recursively query public DNS servers, validate the identity of the DNS server sending the responses, and then cache the responses. You do this by configuring a validating resolver cache on the system. The next time the BIG-IP system receives a query for a response that exists in the cache, the system returns the DNSSEC-compliant response from the cache. The *validating resolver* cache contains messages, resource records, the nameservers the system queries to resolve DNS queries, and DNSSEC keys.

Using the validating resolver cache, the BIG-IP system mitigates cache poisoning by validating DNS responses using DNSSEC validation. This is important, because attackers can attempt to populate a DNS cache with erroneous data that redirects clients to fake web sites, or downloads malware and viruses to client computers. When an authoritative server signs a DNS response, the validating resolver verifies the data before entering the data into the cache. Additionally, the validating resolver cache includes a built-in filter and detection mechanism that rejects unsolicited DNS responses.

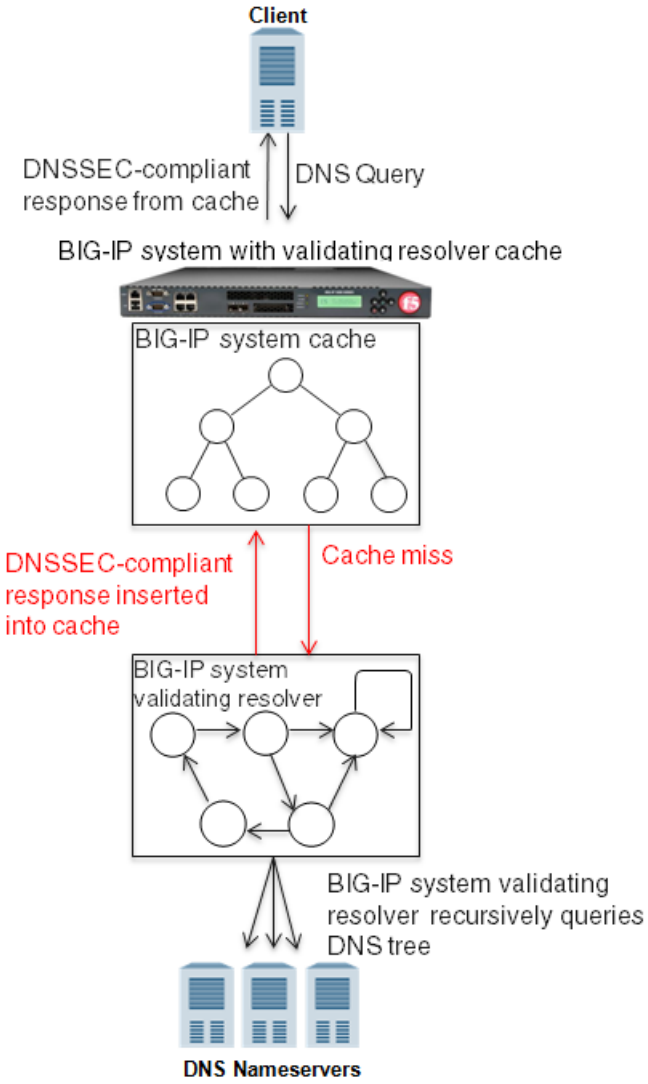


Figure 16: BIG-IP system using validating resolver cache

Task summary

Creating a validating resolver DNS cache
Enabling validating resolver DNS caching
Determining DNS cache performance
Clearing a DNS cache

Creating a validating resolver DNS cache

Create a validating resolver cache on the BIG-IP® system when you want the system to resolve DNS queries, use DNSSEC to validate the responses, and cache the responses.

1. On the Main tab, click **DNS** > **Caches** > **Cache List**.
   The DNS Cache List screen opens.
2. Click **Create**.
   The New DNS Cache screen opens.
3. In the **Name** field, type a name for the cache.

4. From the **Resolver Type** list, select **Validating Resolver**.
5. Click **Finished**.

Associate the DNS cache with a custom DNS profile.

About SEP records and DNSSEC

Each DNSSEC zone has a list of read-only Security Entry Point (SEP) records. The BIG-IP® Global Traffic Manager™ (GTM™) creates these records automatically when you create a zone. These SEP records consist of Delegation Signer (DS) and DNSKEY records.

Obtaining a trust or DLV anchor

Determine the signed zones from which you want to obtain a trust or DLV anchor.

If you want the BIG-IP® system to cache a validated response for the signed zones, you need to obtain a trust or DLV anchor.

1. On the Main tab, click **DNS** > **Zones** > **DNSSEC Zones**.
   The DNSSEC Zone List screen opens.
2. Click the name of the DNSSEC zone for which you want to view or copy SEP records.
3. On the menu bar, click **SEP Records**.
   The SEP records display for each generation of a key. If the SEP record screen is unexpectedly blank, ensure that at least one data center and a server representing the BIG-IP GTM device exist in the BIG-IP system configuration.
4. Copy the trust or DLV anchor from the **DNSKEY Record** field.

Adding a trust anchor to a validating resolver DNS cache

Ensure that you have copied trust anchors for the signed zones that you want to add to the validating resolver.

A validating resolver uses at least one trust anchor to validate DNS responses.

1. On the Main tab, click **DNS** > **Caches** > **Cache List**.
   The DNS Cache List screen opens.
2. Click the name of the cache you want to modify.
   The properties screen opens.
3. On the menu bar, click **Trust Anchors**.
   The Trust Anchors screen opens.
4. Click the **Add** button.
5. In the **Trust Anchor** field, paste the trust anchor that you copied from the signed zone.

   Important: *The trust anchor must be specified in a string format.*

6. Click **Finished**.
7. For each additional trust anchor that you want to add to the validating resolver, repeat steps 4-6.

The validating resolver can now validate the content of DNS responses from the zones for which you added trust anchors.

Adding a DLV anchor to a validating resolver DNS cache

Ensure that you have copied a DLV anchor for the signed zones that you want to add to the validating resolver.

A validating resolver needs a DLV anchor to validate DNS responses from outside a zone.

1. On the Main tab, click **DNS** > **Caches** > **Cache List**.
   The DNS Cache List screen opens.
2. Click the name of the cache you want to modify.
   The properties screen opens.
3. On the menu bar, click **DLV Anchors**.
   The DLV Anchors screen opens.
4. Click the **Add** button.
5. In the **DLV Anchor** field, paste the DLV anchor that you want to add to the validating resolver.

   Important: *The DLV anchor must be specified in a string format.*

6. Click **Finished**.
7. For each additional DLV anchor that you want to add to the validating resolver, repeat steps 4-6.

The validating resolver can now validate the content of DNS responses from the zones for which you added DLV anchors.

Enabling validating resolver DNS caching

Ensure that at least one DNS cache exists on the BIG-IP® system.

To enable the BIG-IP system to validate the identity of the DNS servers returning responses and then to cache those responses, create a custom DNS profile and associate it with a validating resolver DNS cache.

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. In the **Parent Profile** list, accept the default **dns** profile.
5. Select the **Custom** check box.
6. From the **Use BIND Server on BIG-IP** list, select **Disabled**.
7. From the **DNS Cache** list, select **Enabled**.

   When you enable the **DNS Cache** option, you must also select a DNS cache from the **DNS Cache Name** list.
8. From the **DNS Cache Name** list, select the DNS cache that you want to associate with this profile.

   You can associate a DNS cache with a profile, even when the **DNS Cache** option, is **Disabled**.
9. Click **Finished**.

Assign the custom DNS profile to the virtual server that handles the DNS traffic that includes the responses to queries that you want to cache.

Determining DNS cache performance

Ensure that you have created a DNS cache and associated it with a DNS profile, and have assigned the profile to either an LTM® virtual server or a GTM™ listener.

You can view statistics to determine how well a DNS cache on the BIG-IP® system is performing.

1. On the Main tab, click **Statistics** > **Module Statistics** > **DNS** > **Caches**.
   The DNS Caches Status Summary screen opens.
2. From the **Statistics Type** list, select **Caches**.
   Information displays about the DNS caches.

Record type	Description
Queries	Total number of queries handled by the cache.
Responses	Total number of responses sent from the cache.
Sync	Number of synchronous queries handled by the cache.
Async	Number of asynchronous queries handled by the cache.
Resolve	Total number of DNS resolve failures.
Connect	Total number of DNS connect failures.
Server	Number of DNS server failures.
Send	Number of DNS response send failures.

3. In the Details column for a cache, click **View** to display detailed information about the cache.
4. To return to the DNS Cache Statistics screen, click the **Back** button.

Viewing records in a DNS cache

You can view records in a DNS cache to determine how well a specific cache on the BIG-IP® system is performing.

1. Log in to the command-line interface of the BIG-IP system.
2. At the BASH prompt, type the command:
   ```
   tmsh
   ```
3. At the `tmsh` prompt, type the command:
   ```
   show ltm dns cache records rrset cache <cache name>
   ```
   For example, the command: `show ltm dns cache records rrset cache` *`my_transparent_cache`*, displays the resource records in the cache named *`my_transparent_cache`*.

Viewing DNS cache statistics in the Configuration utility

Ensure that you have created a DNS cache and a DNS profile and have assigned the profile to either an LTM® virtual server or a GTM™ listener.

You can view DNS cache statistics to determine how well a specific cache on the BIG-IP® system is performing.

1. On the Main tab, click **Statistics** > **Module Statistics** > **DNS** > **Caches**.
   The DNS Caches Status Summary screen opens.
2. From the **Statistics Type** list, select **Caches**.
3. In the Details column for a cache, click **View** to display detailed information about the cache.
4. To return to the DNS Cache Statistics screen, click the **Back** button.

Viewing DNS cache statistics using tmsh

You can view DNS cache statistics to determine how well a specific cache on the BIG-IP® system is performing.

1. On the Main tab, click **Statistics** > **Module Statistics** > **DNS** > **Caches**.
   The DNS Caches Status Summary screen opens.
2. From the **Statistics Type** list, select **Caches**.
   Information displays about the DNS caches.

Record type	Description
Queries	Total number of queries handled by the cache.
Responses	Total number of responses sent from the cache.
Sync	Number of synchronous queries handled by the cache.
Async	Number of asynchronous queries handled by the cache.
Resolve	Total number of DNS resolve failures.
Connect	Total number of DNS connect failures.
Server	Number of DNS server failures.
Send	Number of DNS response send failures.

3. To return to the DNS Cache Statistics screen, click the **Back** button.

Managing cache size

Determine the amount of memory the BIG-IP® system has and how much you want to commit to DNS caching. View the statistics for a cache to determine how well the cache is working.

You can change the size of a DNS cache to fix cache performance issues.

1. On the Main tab, click **DNS** > **Caches** > **Cache List**.
   The DNS Cache List screen opens.
2. Click the name of the cache you want to modify.
   The properties screen opens.
3. In the **Message Cache Size** field, type the maximum size in bytes for the DNS message cache.

   The BIG-IP system caches the messages in a DNS response in the message cache. A higher maximum size makes it possible for more DNS responses to be cached and increases the cache hit percentage. A lower maximum size forces earlier eviction of cached content, but can lower the cache hit percentage.

Important: *When you change the value of the* ***Message Cache Size****, the records in the message cache are automatically removed. If you do not want to clear the message cache, do not change the value of this parameter.*

4. In the **Resource Record Cache Size** field, type the maximum size in bytes for the DNS resource record cache.

   The BIG-IP system caches the supporting records in a DNS response in the Resource Record cache. A higher maximum size makes it possible for more DNS responses to be cached and increases the cache hit percentage. A lower maximum size forces earlier eviction of cached content, but can lower the cache hit percentage. .

   Warning: *When you change the value of the* ***Resource Record Cache Size****, the records in the resource record cache are automatically removed from the cache. If you do not want to clear the resource record cache, do not change the value of this parameter.*

5. In the **Nameserver Cache Count** field, type the maximum number of DNS nameservers for which the BIG-IP® system caches connection and capability data.

   Important: *When you change the value of the* ***Nameserver Cache Count****, the records in the nameserver cache are automatically removed from the cache. If you do not want to clear the nameserver cache, do not change the value of this parameter.*

6. In the **Unsolicited Reply Threshold** field, change the default value if you are using the BIG-IP® system to monitor for unsolicited replies using SNMP.

   The system always rejects unsolicited replies. The default value of 0 (off) indicates the system does not generate SNMP traps or log messages when rejecting unsolicited replies. Changing the default value alerts you to a potential security attack, such as cache poisoning or DOS. For example, if you specify 1,000,000 unsolicited replies, each time the system receives 1,000,000 unsolicited replies, it generates an SNMP trap and log message.

7. Click **Update**.

Clearing a DNS cache

You can clear all records from a specific DNS cache on the BIG-IP® system.

1. On the Main tab, click **DNS** > **Caches** > **Cache List**.
   The DNS Cache List screen opens.
2. On the menu bar, click **Statistics**.
   The Local Traffic Statistics screen opens.
3. Select the check box next to the cache you want to clear, and then click **Clear Cache**.

Clearing groups of records from a DNS cache

You can clear groups of records of a specific type from a DNS cache by resizing the cache that contains those records.

1. On the Main tab, click **DNS** > **Caches** > **Cache List**.
   The DNS Cache List screen opens.
2. Click the name of the cache you want to modify.

The properties screen opens.

3. In the DNS Cache area, to clear specific records from the cache, do one of the following:

Option	Description
To clear messages from the cache:	change the value in the **Message Cache Size** field.
To clear resource records from the cache:	change the value in the **Resource Record Cache Size** field.
To clear nameservers from the cache:	change the value in the **Name Server Cache Count** field.
To clear DNSSEC keys from the cache:	change the value in the **DNSSEC Key Cache Size** field.

4. Click **Update**.

The BIG-IP® system clears the records in the caches that you resized.

Clearing specific records from a DNS cache using tmsh

You can clear specific records from a DNS cache using `tmsh`. For example, you can delete all RRSET records or only the A records in the specified cache.

Tip: *In `tmsh`, you can use the command completion feature to discover the types of records that are available for deletion.*

1. Log in to the command-line interface of the BIG-IP® system.
2. At the BASH prompt, type the command:
   ```
   tmsh
   ```
3. At the `tmsh` prompt, to navigate to the directory that contains the DNS cache records, type the command:
   ```
   ltm dns cache records
   ```
4. To delete specific DNS cache records, type a variation of this command:
   ```
   delete <cache-type> type <record-type> cache <cache-name>
   ```
   For example, the command `delete rrset type a cache my_resolver_cache`, deletes the A records from the resource record cache of the resolver cache named *my_resolver_cache*.

Overview: Resolving queries for local zones with authoritative responses

You can configure a transparent, resolver, or validating resolver DNS cache with local zones. Use this configuration when you want the BIG-IP® system to resolve queries for small local zones with authoritative responses.

For example, the network administrator at Site Request created a resolver DNS cache to handle DNS traffic for `siterequest.com`. She configured the cache to provide authoritative DNS responses to all domains on the Internet. Now, she wants to configure the cache to serve authoritative responses to queries for the small local zone `wiki.siterequest.com`. When resolving DNS queries for wiki.siterequest.com, the local zone effectively supercedes the cache.

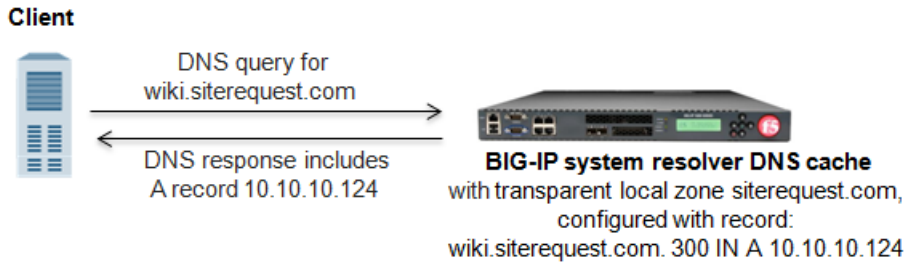


Figure 17: Successful DNS query resolution from transparent local zone

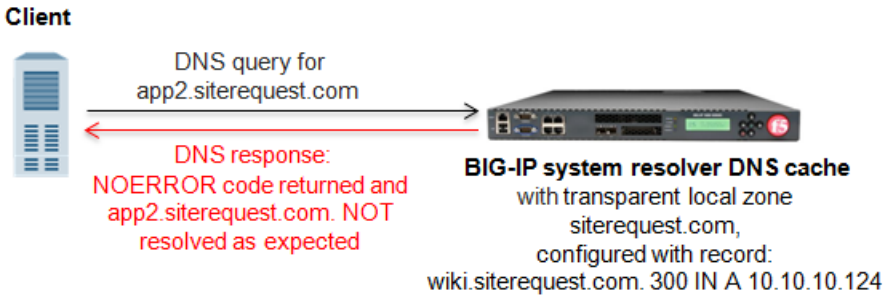


Figure 18: Failed DNS query resolution from transparent local zone

About local zones

A *local zone* contains resource records that a DNS cache uses to resolve matching DNS queries with authoritative DNS responses. The **Type** attribute of the local zone determines how the cache handles a DNS query that does not match the local zone.

Adding local zones to a DNS cache

Ensure that at least one DNS cache is configured on the BIG-IP® system.

Determine which local zones and associated resource records you want the BIG-IP system to respond to with authoritative DNS responses.

Add a local zone to a DNS cache only when the zone has a small resource record set.

Tip: *If you want the BIG-IP system to respond to DNS queries with authoritative DNS responses for a zone with a large resource record set, instead create a DNS zone and enable DNS Express™.*

---

1. On the Main tab, click **DNS** > **Caches** > **Cache List**.
   The DNS Cache List screen opens.
2. Click the name of the cache you want to modify.
   The properties screen opens.
3. On the menu bar, click **Local Zones**.
   The Local Zones screen opens.
4. Click the **Add** button.
5. In the **Name** field, type the domain name of the local zone.

Note: *The domain you enter must be at the apex of the zone. For example, you could name a local zone* `siterequest.com`*, and then add resource records for the members* `wiki.siterequest.com.` *and* `download.siterequest.com.`*.*

6. From the **Type** list, select how the cache handles a non-matching query for the local zone.

Tip: *The Description column provides a sample response to a query for* `example.com`*, when the local zone is* `siterequest.com`*.*

Option	Description
Deny	For a non-matching query, the cache drops the DNS query. This is an example of a response to a non-matching query: `DNS request timed out`
Redirect	For a non-matching query, when the query is for a subdomain of the local zone, the cache returns the same response that it would for the local zone. For example, if you add the local zone `siterequest.com`, the cache returns the same response to queries for `wiki.siterequest.com.` and `download.wiki.siterequest.com.`. This is an example of a response to a non-matching query: `NOERROR rcode returned and example.com. NOT resolved as expected`
Refuse	For a non-matching query, the cache returns a REFUSED message in the DNS response. This is an example of a response to a non-matching query: `REFUSED rcode returned and example.com. NOT resolved as expected`
Static	For a non-matching query, the cache returns a NoData or NXDOMAIN in the DNS response, which also includes the SOA record if the local zone contains one. This is an example of a response to a non-matching query: `NOERROR rcode returned and example.com. NOT resolved as expected`
Transparent	**Transparent** is the default value. For a non-matching query, the cache performs a pass-through or iterative resolution of the DNS query. If the query matches, but no resource records are available, the cache returns a response with a NoData message. This is an example of a response to a non-matching query: `NOERROR rcode returned and example.com. NOT resolved as expected`
Type Transparent	For a non-matching query, or a query for a matching domain name, but with a request for a record of a different type, the cache performs a pass-through or iterative resolution of the DNS query; however, if the query matches, but no resource records are available, the cache does not return a response with a NoData message. This is an example of a response to a non-matching query: `DNS request resolved to example.com. as expected`

7. In the Records area, in the field, specify a resource record to identify the local zone, including domain name, type, class, TTL, and record data, separated by spaces, and then click **Add**.

Note: *You can add multiple resource records.*

This is an example of an A record entry: `wiki.siterequest.com. 300 IN A 10.10.10.124`. This is an example of a AAAA record entry: `wiki.siterequest.com. 300 IN AAAA 2002:0:1:12:123:c:cd:cdf`.

8. Click **Finished**.

Overview: Forwarding specific DNS queries to specific nameservers

You can configure a resolver or validating resolver DNS cache with forward zones. Do this configuration when you want the BIG-IP® system to forward DNS queries that match the forward zones to specific nameservers, which resolve the query when the cache does not contain a response.

For example, the network administrator for Site Request wants to configure the DNS cache to resolve responses to queries for the zone: `app1.siterequest.com`. She wants the responses to queries for this zone to be served from specific nameservers, when the cache does not contain a response.

Figure 19: Successful DNS query resolution from forward zone

Important: *When a DNS cache configured with both local and forward zones receives a DNS query, the system checks the local zones first. If the query does not match a local zone, the system then checks the forward zones for a match.*

About forward zones

A DNS cache *forward zone* resolves matching DNS queries by obtaining answers from one of the recursive nameservers associated with the forward zone. When the BIG-IP® system receives a query that cannot be resolved from the cache, the system forwards the query to a nameserver associated with the matching forward zone. When the nameserver returns a response, the BIG-IP system caches the response, and returns the response to the resolver making the query.

Longest match

The BIG-IP system matches a DNS query with a forward zone based on longest match. For example, the network administrator for Site Request, configures two forward zones. `download.siterequest.com.` is configured with two nameservers with the IP addresses `172.27.5.1` and `172.27.7.247`. `app1.siterequest.com.` is configured with two nameservers with the IP addresses `10.10.5.5` and `11.11.5.7`. A query for `product.download.siterequest.com.` matches the forward zone `download.siterequest.com` and a query for `ftp.appl1.siterequest.com.` matches the forward zone `app1.siterequest.com`.

Selecting a nameserver

When a forward zone is configured with more than one nameserver, the BIG-IP system forwards the first query to a randomly selected nameserver, and records the round trip time (RTT) of a successful response. If the first nameserver does not return a response, the BIG-IP system forwards the query to a different nameserver and records the RTT of a successful response. After that, the system always sends a query to the nameserver with the fastest RTT. If none of the nameservers return a response, or the RTT exceeds 120 seconds, the BIG-IP system returns a `SERVFAIL` response to the resolver making the query.

Task summary

Perform these tasks to configure the BIG-IP® system to forward DNS queries to specific DNS servers.

Adding forward zones to a DNS cache
Deleting forward zones from a DNS cache
Changing the nameservers associated with a forward zone
Viewing statistics about DNS cache forward zones

Adding forward zones to a DNS cache

Ensure that at least one resolver DNS cache or validating resolver DNS cache exists in the configuration.

Gather the IP addresses of the nameservers that you want to associate with a forward zone.

When you want the BIG-IP® system to forward queries to specific nameservers for resolution and the cache does not contain a response to the query, add a forward zone to a DNS cache.

1. On the Main tab, click **DNS** > **Caches** > **Cache List**.
   The DNS Cache List screen opens.
2. Click the name of the cache you want to modify.
   The properties screen opens.
3. On the menu bar, click **Forward Zones**.
   The Forward Zones screen opens.
4. Click the **Add** button.
5. In the **Name** field, type a name for the forward zone.
6. In the Nameservers area, in the **Address** field, type the IP address of a DNS nameserver that the system considers authoritative for this zone, and then click **Add**. Based on your network configuration, add IPv4 or IPv6 addresses, or both.

   Note: *The order of nameservers in the configuration does not impact which nameserver the system selects to forward a query to.*

7. Click **Finished**.

Deleting forward zones from a DNS cache

Determine which forward zone you want to delete.

When you no longer want the BIG-IP® system to forward queries to a forward zone, you can delete the forward zone.

1. On the Main tab, click **DNS** > **Caches** > **Cache List**.
   The DNS Cache List screen opens.
2. Click the name of the cache you want to modify.
   The properties screen opens.
3. On the menu bar, click **Forward Zones**.
   The Forward Zones screen opens.
4. Select the check box next to the forward zone you want to delete, and then click **Delete**.
   A dialog box displays asking you to confirm the deletion.
5. Click **OK** to confirm the deletion.

Changing the nameservers associated with a forward zone

Determine the forward zone that you want to modify.

Modify the nameservers that are associated with a forward zone when you want the BIG-IP® system to forward DNS queries for a matching forward zone to a different set of nameservers.

1. On the Main tab, click **Local Traffic** > **DNS Caches** > **DNS Cache List**.
   The DNS Cache List screen opens.
2. Click the name of the cache you want to modify.
   The properties screen opens.
3. On the menu bar, click **Forward Zones**.
   The Forward Zones screen opens.
4. Click the name of the forward zone you want to modify.
   The properties screen opens.
5. In the Nameservers area, add or remove nameservers.
6. Click **Finished**.

Viewing statistics about DNS cache forward zones

Ensure that at least one DNS cache exists in the BIG-IP® system configuration.

You can view statistics about the queries and responses that a DNS cache forwards. For example, to assess the reliability of a nameserver, you can view data about the number of queries resolved by the nameserver within a specified timeframe.

1. On the Main tab, click **Statistics** > **Module Statistics** > **DNS** > **Caches**.
   The DNS Caches Status Summary screen opens.
2. From the **Statistics Type** list, select **Caches**.
3. In the Details column for a cache, click **View** to display detailed information about the cache.
4. View the statistics in the Forwarder Activity area.

Overview: Forwarding specific DNS queries to a pool of DNS servers

You can configure a resolver or validating resolver DNS cache with a forward zone that is associated with a listener. The listener can load balance specific DNS queries to a pool of DNS servers. For example, the

network administrator for Site Request wants to configure the DNS cache to resolve DNS queries for the forward zone `app2.siterequest.com`, and wants the responses to be served from a pool of local DNS servers, when the cache does not contain a response.

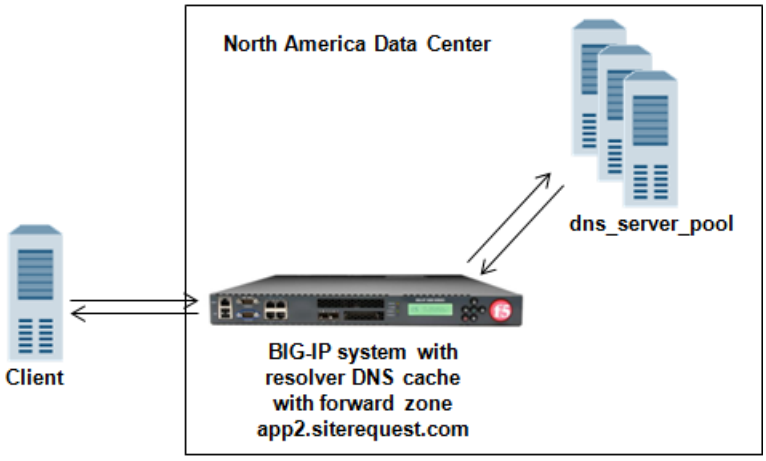


Figure 20: Successful DNS query resolution from pool of DNS servers associated with a forward zone

Task summary

Creating a custom DNS monitor
Creating a pool of local DNS servers
Creating a resolver DNS cache
Enabling resolving and caching
Creating listeners that alert GTM to DNS queries for a pool of DNS servers
Configuring a forward zone with a listener that load balances DNS queries

Creating a custom DNS monitor

Create a custom DNS monitor to send DNS queries, generated using the settings you specify, to a pool of DNS servers and validate the DNS responses.

Important: *When defining values for custom monitors, make sure you avoid using any values that are on the list of reserved keywords. For more information, see SOL 3653 (for version 9.0 systems and later) on the AskF5™ technical support web site at* `www.askf5.com`.

---

1. On the Main tab, click **DNS** > **Delivery** > **Load Balancing** > **Monitors** or **Local Traffic** > **Monitors**.
   The Monitor List screen opens.
2. Click **Create**.
   The New Monitor screen opens.
3. Type a name for the monitor in the **Name** field.
4. From the **Type** list, select **DNS**.
5. In the **Query Name** field, type the domain name that you want the monitor to query.
   For the zone, `siterequest.com`, you might want the monitor to query for `www.siterequest.com`.
6. Configure additional settings based on your network requirements.
7. Click **Finished**.

Creating a pool of local DNS servers

Ensure that at least one custom DNS monitor exists on the BIG-IP® system. Gather the IP addresses of the DNS servers that you want to include in a pool to which the BIG-IP system load balances DNS traffic.

Create a pool of local DNS servers when you want to load balance DNS queries to other DNS servers.

1. On the Main tab, click **DNS** > **Delivery** > **Load Balancing** > **Pools** or **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 custom DNS monitor you created, and click **<<** to move the monitor to the **Active** list.
5. Using the **New Members** setting, add each resource that you want to include in the pool:
   a) Type an IP address in the **Address** field.
   b) Type a port number in the **Service Port** field, or select a service name from the list.
   c) To specify a priority group, type a priority number in the **Priority Group Activation** field.
   d) Click **Add**.
6. Click **Finished**.

Creating a resolver DNS cache

Create a resolver cache on the BIG-IP® system when you want the system to resolve DNS queries and cache responses.

1. On the Main tab, click **DNS** > **Caches** > **Cache List**.
   The DNS Cache List screen opens.
2. Click **Create**.
   The New DNS Cache screen opens.
3. In the **Name** field, type a name for the cache.
4. From the **Resolver Type** list, select **Resolver**.
5. Click **Finished**.

Associate the DNS cache with a custom DNS profile.

Enabling resolving and caching

Ensure that at least one DNS cache exists on the BIG-IP® system.

To enable the BIG-IP system to resolve DNS queries and cache the responses, create a custom DNS profile and associate it with a resolver DNS cache.

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. From the **Use BIND Server on BIG-IP** list, select **Disabled**.
6. From the **DNS Cache** list, select **Enabled**.
   When you enable the **DNS Cache** option, you must also select a DNS cache from the **DNS Cache Name** list.
7. From the **DNS Cache Name** list, select the DNS cache that you want to associate with this profile.
   You can associate a DNS cache with a profile, even when the **DNS Cache** option, is **Disabled**.
8. Click **Finished**.

Assign the custom DNS profile to the virtual server or listener that handles the DNS traffic.

Creating listeners that alert GTM to DNS queries for a pool of DNS servers

Ensure that a pool of DNS servers exists on GTM™.

Configure a listener that alerts GTM to DNS queries destined for a pool of DNS servers. The best practice is to create four listeners: one with an IPv4 address that handles UDP traffic, and one with the same IPv4 address that handles TCP traffic; one with an IPv6 address that handles UDP traffic, and one with the same IPv6 address that handles TCP traffic.

Tip: *If you have multiple GTM systems in a device group, perform this procedure on only one system.*

---

1. On the Main tab, click **DNS** > **Delivery** > **Listeners**.
   The Listeners List screen opens.
2. Click **Create**.
   The Listeners properties screen opens.
3. In the **Name** field, type a unique name for the listener.
4. For the Destination setting, in the **Address** field, type an IPv4 address on which GTM listens for network traffic.
5. From the **Listener** list, select **Advanced**.
6. For the **Address Translation** setting, select the **Enabled** check box.
7. In the Service area, from the **Protocol** list, select **UDP**.
8. From the **Default Pool** list, select the pool to which this listener forwards DNS queries.
9. Click **Finished**.

Create another listener with the same IPv4 address and configuration, but select **TCP** from the **Protocol** list. Then, create two more listeners, configuring both with the same IPv6 address, but one with the UDP protocol and one with the TCP protocol.

Configuring a forward zone with a listener that load balances DNS queries

Determine the DNS cache to which you want to add a forward zone. Ensure that a listener that is associated with a pool of DNS servers is configured on the system.

When you want the BIG-IP® GTM™ to forward DNS queries to a pool of DNS servers, configure a forward zone with a nameserver that is a listener, which load balances traffic to a pool of DNS servers.

1. On the Main tab, click **DNS** > **Caches** > **Cache List**.

The DNS Cache List screen opens.

2. Click the name of the cache you want to modify.
   The properties screen opens.
3. On the menu bar, click **Forward Zones**.
   The Forward Zones screen opens.
4. Click the **Add** button.
5. In the **Name** field, type a name for the forward zone.
6. In the Nameservers area, in the **Address** field, type the IP address of a DNS nameserver that the system considers authoritative for this zone, and then click **Add**. Based on your network configuration, add IPv4 or IPv6 addresses, or both.

   Note: *The order of nameservers in the configuration does not impact which nameserver the system selects to forward a query to.*

7. Click **Finished**.

Depending upon your network configuration, add additional listeners to the forward zone. The best practice is to associate four listeners with the forward zone: one with an IPv4 address that handles UDP traffic, and one with the same IPv4 address that handles TCP traffic; one with an IPv6 address that handles UDP traffic, and one with the same IPv6 address that handles TCP traffic.

Overview: Customizing a DNS cache

You can customize a DNS cache on the BIG-IP® system to meet specific network needs by changing the default values on the DNS cache settings.

Resolving DNS queries for default local zones from a DNS cache

You can configure a DNS cache on the BIG-IP® system to answer DNS queries for default local zones.

1. On the Main tab, click **DNS** > **Caches** > **Cache List**.
   The DNS Cache List screen opens.
2. Click the name of the cache you want to modify.
   The properties screen opens.
3. Select the **Enabled** check box for the **Answer Default Zones** setting, when you want the BIG-IP® system to answer queries for the default zones: localhost, reverse 127.0.0.1 and ::1, and AS112 zones.
4. Click **Update**.

Using specific DNS servers as authoritative root nameservers

You can configure a resolver or validating resolver DNS cache on the BIG-IP® system to use a specific server as an authoritative nameserver for the DNS root nameservers.

1. On the Main tab, click **DNS** > **Caches** > **Cache List**.
   The DNS Cache List screen opens.
2. Click the name of the cache you want to modify.

The properties screen opens.

3. In the **Root Hints** area, in the **IP address** field, type the IP address of a DNS server that the system considers authoritative for the DNS root nameservers, and then click **Add**.

Caution: *By default, the system uses the DNS root nameservers published by InterNIC. When you add DNS root nameservers, the BIG-IP system no longer uses the default nameservers published by InterNIC, but uses the nameservers you add as authoritative for the DNS root nameservers.*

Based on your network configuration, add IPv4 or IPv6 addresses or both.

4. Click **Update**.

Alerting the system to cache poisoning

You can configure a resolver or validating resolver DNS cache on the BIG-IP® system to generate SNMP alerts and log messages when the cache receives unsolicited replies. This is helpful as an alert to a potential security attack, such as cache poisoning or DDoS.

1. On the Main tab, click **DNS** > **Caches** > **Cache List**.
   The DNS Cache List screen opens.
2. Click the name of the cache you want to modify.
   The properties screen opens.
3. In the **Unsolicited Reply Threshold** field, change the default value if you are using the BIG-IP® system to monitor for unsolicited replies using SNMP.

   The system always rejects unsolicited replies. The default value of 0 (off) indicates the system does not generate SNMP traps or log messages when rejecting unsolicited replies. Changing the default value alerts you to a potential security attack, such as cache poisoning or DOS. For example, if you specify 1,000,000 unsolicited replies, each time the system receives 1,000,000 unsolicited replies, it generates an SNMP trap and log message.
4. Click **Update**.

Chapter 6

Configuring DNS64

Overview: Configuring DNS64

You can configure BIG-IP® Local Traffic Manager™ (LTM®) and BIG-IP® Global Traffic Manager™ (GTM™) systems to handle IPv6-only client connection requests to IPv4-only servers on your network by returning an AAAA record response to the client.

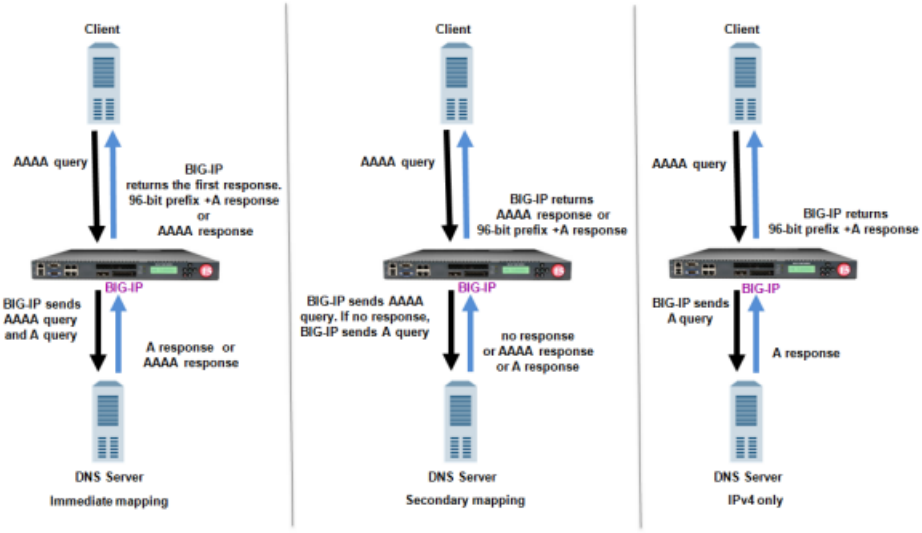


Figure 21: Mapping IPv6 addresses to IPv4 addresses

Task summary

Creating a custom DNS profile
Assigning a DNS profile to a DNS listener
Assigning a DNS profile to a virtual server

Creating a custom DNS profile

You can create a custom DNS profile to configure how the BIG-IP® system handles DNS queries.

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. In the **Parent Profile** list, accept the default **dns** profile.
5. Select the **Custom** check box.
6. In the **Global Traffic Management** list, accept the default value **Enabled**.
7. From the **DNS IPv6 to IPv4** list, select how you want the system to handle IPv6 to IPv4 address mapping in DNS queries and responses.

Option	Description
Disabled	The BIG-IP system does not map IPv4 addresses to IPv6 addresses.

Option	Description
Immediate	The BIG-IP system receives an AAAA query and forwards the query to a DNS server. The BIG-IP system then forwards the first good response from the DNS server to the client. If the system receives an A response first, it appends a 96-bit prefix to the record and forwards it to the client. If the system receives an AAAA response first, it simply forwards the response to the client. The system disregards the second response from the DNS server.
Secondary	The BIG-IP system receives an AAAA query and forwards the query to a DNS server. Only if the server fails to return a response does the BIG-IP system send an A query. If the BIG-IP system receives an A response, it appends a 96-bit user-configured prefix to the record and forwards it to the client.
v4 Only	The BIG-IP system receives an AAAA query, but forwards an A query to a DNS server. After receiving an A response from the server, the BIG-IP system appends a 96-bit user-configured prefix to the record and forwards it to the client.

Important: *Select this option only if you know that all your DNS servers are IPv4 only servers.*

If you selected **Immediate**, **Secondary**, or **V4 Only** two new fields display.

8. In the **IPv6 to IPv4 Prefix** field, specify the prefix the BIG-IP system appends to all A query responses to an IPv6 request.
9. From the **IPv6 to IPv4 Additional Section Rewrite** list, select an option to allow improved network efficiency for both Unicast and Multicast DNS-SD responses.

Option	Description
Disabled	The BIG-IP system does not perform additional rewrite.
v4 Only	The BIG-IP system accepts only A records. The system appends the 96-bit user-configured prefix to a record and returns an IPv6 response to the client.
v6 Only	The BIG-IP system accepts only AAAA records and returns an IPv6 response to the client.
Any	The BIG-IP system accepts and returns both A and AAAA records. If the DNS server returns an A record in the Additional section of a DNS message, the BIG-IP system appends the 96-bit user-configured prefix to the record and returns an IPv6 response to the client.

10. From the **Use BIND Server on BIG-IP** list, select **Enabled**.

Note: *Enable this setting only when you want the system to forward non-wide IP queries to the local BIND server on BIG-IP GTM.*

11. Click **Finished**.

Assigning a DNS profile to a DNS listener

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 the profile you created to manage IPv6 to IPv4 address mapping.

4. Click **Update**.

This listener can now pass traffic between an IPv6-only client and an IPv4-only DNS server.

Assigning a DNS profile to a virtual server

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 the profile you created to manage IPv6 to IPv4 address mapping.
5. Click **Update**.

This virtual server can now pass traffic between an IPv6-only client and an IPv4-only DNS server.

Implementation result

You now have an implementation of DNS64 on the BIG-IP® system.

Chapter 7

Configuring IP Anycast (Route Health Injection)

Overview: Configuring IP Anycast (Route Health Injection)

You can configure IP Anycast for DNS services on the BIG-IP® system to help mitigate distributed denial-of-service attacks (DDoS), reduce DNS latency, improve the scalability of your network, and assist with traffic management. This configuration adds routes to and removes routes from the routing table based on availability. Advertising routes to virtual addresses based on the status of attached listeners is known as *Route Health Injection (RHI)*.

Task Summary

Enabling the ZebOS dynamic routing protocol

Before you enable ZebOS® dynamic routing on the BIG-IP® system:

- Ensure that the system license includes the Routing Bundle add-on.
- Ensure that ZebOS is configured correctly. If you need help, refer to the following resources on AskF5®:
  - *BIG-IP®TMOS®: Concepts*
  - *BIG-IP®TMOS®: Implementations*
  - *BIG-IP®TMOS®: IP Routing Administration*
  - *BIG-IP® Advanced Routing* (multiple manuals are available)

Enable ZebOS protocols to allow the BIG-IP system to dynamically learn routes.

1. Log on to the command-line interface of the BIG-IP system.
2. At the command prompt, type `zebos enable <protocol_type>` and press Enter.
   The system returns an enabled response.
3. To verify that the ZebOS dynamic routing protocol is enabled, at the command prompt, type `zebos check` and press Enter.
   The system returns a list of all enabled protocols.

Creating a custom DNS profile

Create a custom DNS profile based on your network configuration, to specify how you want the BIG-IP® system to handle non-wide IP DNS queries.

1. On the Main tab, click **DNS** > **Delivery** > **Profiles** > **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. In the **Parent Profile** list, accept the default **dns** profile.
5. Select the **Custom** check box.

6. In the **Global Traffic Management** list, accept the default value **Enabled**.
7. From the **Unhandled Query Actions** list, select how you want the BIG-IP system to handle a query that is not for a wide IP or DNS Express zone.

Option	Description
Allow	The BIG-IP system forwards the query to a DNS server or a member of a pool of DNS servers. Note that if the pool is not associated with a listener and the **Use BIND Server on BIG-IP** option is set to **enabled**, queries are forwarded to the local BIND server. (Allow is the default value.)
Drop	The BIG-IP system does not respond to the query.
Reject	The BIG-IP system returns the query with the REFUSED return code.
Hint	The BIG-IP system returns the query with a list of root name servers.
No Error	The BIG-IP system returns the query with the NOERROR return code.

8. From the **Use BIND Server on BIG-IP** list, select **Enabled**.

Note: *Enable this setting only when you want the system to forward non-wide IP queries to the local BIND server on BIG-IP GTM.*

9. Click **Finished**.

Configuring a listener for route advertisement

Ensure that ZebOS® dynamic routing is enabled on BIG-IP® Global Traffic Manager™ (GTM™).

To allow BIG-IP GTM to advertise the virtual address of a listener to the routers on your network, configure the listener for route advertisement.

1. On the Main tab, click **DNS** > **Delivery** > **Listeners**.
   The Listeners List screen opens.
2. Click **Create**.
   The Listeners properties screen opens.
3. In the **Name** field, type a unique name for the listener.
4. For the Destination setting, in the **Address** field, type the IP address on which GTM listens for network traffic.

Caution: *The destination cannot be a self IP address on the system, because a listener with the same IP address as a self IP address cannot be advertised.*

5. From the **VLAN Traffic** list, select **All VLANs**.
6. From the **Listener** list, select **Advanced**.
7. For the **Route Advertisement** setting, select the **Enabled** check box.
8. In the Service area, from the **Protocol** list, select **UDP**.
9. From the **DNS Profile** list, select:

Option	Description
dns	This is the default DNS profile. With the default **dns** profile, GTM forwards non-wide IP queries to the BIND server on the GTM system itself.

Option	Description
<custom profile>	If you have created a custom DNS profile to handle non-wide IP queries in a way that works for your network configuration, select it.

10. Click **Finished**.

Verifying advertisement of the route

Ensure that ZebOS® dynamic routing is enabled on the BIG-IP® system.

Run a command to verify that the BIG-IP system is advertising the virtual address.

1. Log on to the command-line interface of the BIG-IP system.
2. At the command prompt, type `zebos cmd sh ip route | grep <listener IP address>` and press Enter.
   An advertised route displays with a code of K and a 32 bit kernel, for example: `K 127.0.0.1/32`

Implementation result

You now have an implementation in which the BIG-IP® system broadcasts virtual IP addresses that you configured for route advertisement.

Chapter 8

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 to create in implementation	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.

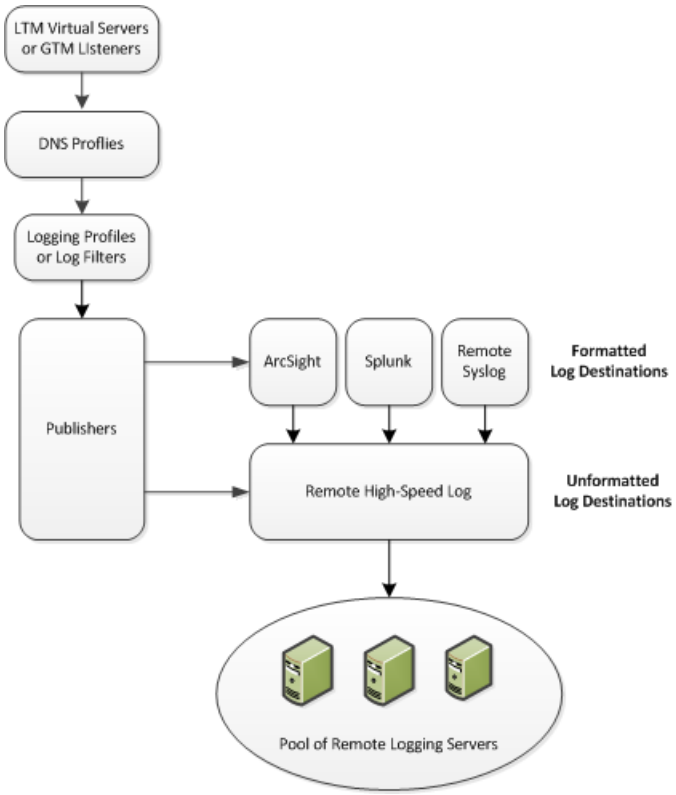


Figure 22: Association of remote high-speed logging configuration objects

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 **DNS** > **Delivery** > **Load Balancing** > **Pools** or **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.*

   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.
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. From the **Logging** list, select **Enabled**.
6. 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. 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.

Chapter 9

Setting Up and Viewing DNS Statistics

Overview: Setting up and viewing DNS statistics

You can view DNS AVR and DNS global statistics on the BIG-IP® system to help you manage and report on the DNS traffic on your network.

DNS AVR Statistics

You must configure an AVR sampling rate on a DNS profile and assign it to a listener or virtual server before the BIG-IP system can gather DNS AVR statistics. An AVR Analytics profile is not required for the BIG-IP system to gather and display DNS AVR statistics. The DNS AVR statistics include DNS queries per:

- Application
- Virtual server
- Query name
- Query type
- Client IP address
- (You can also filter the statistics by time period.)

DNS Global Statistics

The BIG-IP system automatically collects DNS global statistics about the DNS traffic the system processes. The DNS global statistics include:

- Total DNS queries and responses
- Details about DNS queries and responses
- Details about DNS Services rate-limited license
- The number of wide IP requests
- Details about GTM rate-limited license
- The number of DNS Express™ requests and NOTIFY announcements and messages
- The number of DNS cache requests
- The number of DNS IPv6 to IPv4 requests, rewrites, and failures
- The number of unhandled query actions per specific actions

Task Summary

Creating a DNS profile for AVR statistics collection
Viewing DNS AVR statistics
Viewing DNS AVR statistics in tmsh
Viewing DNS global statistics
Viewing DNS statistics for a specific virtual server

Creating a DNS profile for AVR statistics collection

Ensure that Application Visibility and Reporting (AVR) is provisioned.

Configure the BIG-IP® system to collect AVR statistics on a sampling of the DNS traffic that the BIG-IP system handles.

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. Select the **AVR Statistics Sample Rate** check box.
   The **Enabled 1/ 1 queries sampled** field displays.
6. In the **Enabled 1/ 1 queries sample** field, change the `1` to the number of queries from which the system takes one sample.

Option	Description
0	No DNS requests are stored in the Analytics database.
1	All DNS requests are stored in the Analytics database.
n>1	Every nth DNS request is stored in the Analytics database.

7. Click **Finished**.

Assign the DNS profile to a listener or virtual server.

Viewing DNS AVR statistics

Ensure that Application Visibility and Reporting (AVR) is provisioned. Ensure that the BIG-IP® system is configured to collect DNS statistics on a sampling of the DNS traffic that the BIG-IP system handles.

View DNS AVR statistics to help you manage the DNS traffic on your network.

1. On the Main tab, click **Statistics** > **Analytics** > **DNS**.
   The DNS Analytics screen opens.
2. From the **View By** list, select the specific network object type for which you want to display statistics.
   You can also click **Expand Advanced Filters** to filter the information that displays.
3. From the **Time Period** list, select the amount of time for which you want to view statistics.

Tip: *To display reports for a specific time period, select* ***Custom*** *and specify beginning and end dates.*

4. Click **Export** to create a report of this information.

Note: *The timestamp on the report reflects a publishing interval of five minutes; therefore, a time period request of 12:40-13:40 actually displays data between 12:35-13:35. By default, the BIG-IP system displays one hour of data.*

Viewing DNS AVR statistics in tmsh

Ensure that Application Visibility and Reporting (AVR) is provisioned. Ensure that the BIG-IP® system is configured to collect DNS statistics on a sampling of the DNS traffic that the BIG-IP system handles.

View DNS analytics statistics to help you manage the DNS traffic on your network.

1. Log on to the command-line interface of the BIG-IP system.
2. At the BASH prompt, type `tmsh`.
3. At the `tmsh` prompt, type one of these commands and then press Enter.

Option	Description
`show analytics dns report view-by query-name limit 3`	Displays the three most common query names.
`show analytics dns report view-by query-type limit 3`	Displays the three most common query types.
`show analytics dns report view-by client-ip limit 3`	Displays the three client IP addresses from which the most DNS queries originate.
`show analytics dns report view-by query-name drilldown { { entity query-type values {A}}} limit 3`	Displays the three most common query names for query type A records.
`show analytics dns report view-by query-type drilldown { { entity query-name values {www.f5.com}}} limit 3`	Displays the three most common query types for query name `www.f5.com`.
`show analytics dns report view-by client-ip drilldown { { entity query-type values {A}}} limit 3`	Displays the three most common client IP addresses requesting query type A records.

Viewing DNS global statistics

Ensure that at least one DNS profile exists on the BIG-IP® system and that this profile is assigned to an LTM® virtual server or a GTM™ listener that is configured to use the TCP protocol.

Note: *If you want to view AXFR and IXFR statistics, the listener or virtual server must be configured to use the TCP protocol. This is because zone transfers occur over the TCP protocol.*

View DNS global statistics to determine how to fine-tune your network configuration or troubleshoot DNS traffic processing problems.

1. On the Main tab, click **Statistics** > **Module Statistics** > **DNS** > **Delivery**.
   The DNS Delivery statistics screen opens.
2. From the **Statistics Type** list, select **Profiles**.
3. In the Global Profile Statistics area, in the Details column of the DNS profile, click **View**.

Viewing DNS statistics for a specific virtual server

Ensure that at least one virtual server associated with a DNS profile exists on the BIG-IP® system.

Note: *If you want to view AXFR and IXFR statistics, the virtual server must be configured to use the TCP protocol. This is because zone transfers occur over the TCP protocol.*

You can view DNS statistics per virtual server when you want to analyze how the BIG-IP system is handling specific DNS traffic.

1. On the Main tab, click **Statistics** > **Module Statistics** > **Local Traffic**.
   The Local Traffic statistics screen opens.

2. From the **Statistics Type** list, select **Virtual Servers**.
3. In the Details column for the virtual server, click **View**.

Implementation result

You now have an implementation in which the BIG-IP® system gathers both DNS AVR and DNS global statistics. You can view these statistics to help you understand DNS traffic patterns and manage the flow of your DNS traffic, especially when your network is under a DDoS attack.

Chapter 10

Using ZoneRunner to Configure DNS Zones

About ZoneRunner

You can use the ZoneRunner™ utility to create and manage DNS zone files and configure the BIND instance on BIG-IP® Global Traffic Manager™ (GTM™). With the ZoneRunner utility, you can:

- Import and transfer DNS zone files
- Manage zone resource records
- Manage views
- Manage a local nameserver and the associated configuration file, `named.conf`
- Transfer zone files to a nameserver
- Import only primary zone files from a nameserver

About named.conf

`named.conf` contains the primary operational characteristics of BIND, including DNS views, access control list definitions, and zones. The ZoneRunner™ utility updates `named.conf` when you modify the local BIND instance.

Using ZoneRunner to configure named.conf

Ensure that at least one zone is configured on BIG-IP ®GTM™.

Use ZoneRunner™ to edit `named.conf`, to decrease the risk of a syntax error that prevents the BIND system from performing as expected. Zonerunner provides an automatic syntax check and displays error messages to help you write the correct syntax.

1. On the Main tab, click **DNS** > **Zones** > **ZoneRunner** > **named Configuration**.
   The named Configuration screen opens.
2. In the Options area, type additional configurations per your network design.
3. Click **Update**.

Creating a master DNS zone

A master zone is authoritative. Create a zone when you want to use ZoneRunner™ to manage DNS zones and resource records.

Tip: *The BIG-IP® system can be either a primary or secondary DNS server.*

1. On the Main tab, click **DNS** > **Zones** > **ZoneRunner** > **Zone List**.
   The Zone List screen opens.
2. Click **Create**.
   The New Zone screen opens.
3. From the **View Name** list, select **external**.
   The external view is a default view to which you can assign zones.
4. In the **Zone Name** field, type a period character (**.**).
5. From the **Zone Type** list, select **Master**.

6. Clear the **Zone File Name** field, and type the zone file name.
   `db.external.siterequest.com`

   Note: *Do not include a trailing dot.*

7. In the Records Creation area, type the values for the SOA and NS record parameters.
8. Click **Finished**.

If you want further help creating a custom zone file, see *SOL8380* on `www.askf5.com` for instructions.

Creating a hint zone

Hint zones designate a subset of the root nameservers list. When the local nameserver starts (or restarts), the nameserver queries the root servers in the hint zone for the most current list of root servers. The root hint is built into BIND version 9.0 and later.

Create a zone when you want to use ZoneRunner™ to manage DNS zones and resource records.

Tip: *The BIG-IP® system can be either a primary or secondary DNS server.*

1. On the Main tab, click **DNS** > **Zones** > **ZoneRunner** > **Zone List**.
   The Zone List screen opens.
2. Click **Create**.
   The New Zone screen opens.
3. From the **View Name** list, select **external**.
   The external view is a default view to which you can assign zones.
4. In the **Zone Name** field, type a period character (`.`).
5. From the **Zone Type** list, select **Hint**.
6. Clear the **Zone File Name** field, and type the zone file name.
   `db.external.siterequest.com`

   Note: *Do not include a trailing dot.*

7. Click **Finished**.

If you want further help creating a custom hint file, see *SOL8380* on `www.askf5.com` for instructions.

Configuring GTM to allow zone file transfers

By default, BIG-IP® GTM™ is configured to secure BIND to not allow zone transfers except from the localhost. However, you can configure BIG-IP GTM to allow zone file transfers to other DNS servers.

1. On the Main tab, click **DNS** > **Zones** > **ZoneRunner** > **named Configuration**.
   The named Configuration screen opens.
2. In the **Options** field, modify the allow-transfer statement to include the IP address of the GTM.
   You can modify the following allow-transfer statement to use the IP address of the GTM.

```
allow-transfer {
```

```
      localhost;

      192.168.10.105;

      };
```

3. On the menu bar, click **View List**.
   The View List screen opens.
4. Click the name of the view that contains the zone you are configuring.
   The View Configuration screen opens.
5. In the Options area, modify the match-clients statement based on your configuration.

View configuration type	Add to match-clients statement
Single view configuration	`view "external" { match-clients { "zrd-acl-000-000"; any; }; }`
Multiple view configuration, where you want to allow transfers from GTM	Modify the following match-clients statement to use the IP address of the GTM.

```
acl "internal-acl"
     { <IP address> ;
     };

view "internal" {
  match-clients {
    "zrd-acl-000-001";
    "internal-acl";
    <IP address> ;
  };

view "external" {
  match-clients {
    "zrd-acl-000-000";
    any;
  };
```

6. Click **Update**.

To verify that zone transfers are working properly, modify this Linux command and run it on an external computer:`dig @<IP address> es.net. axfr`

The command should return a response similar to this:

```
; <<>> DiG? 9.5.0-P2 <<>> @192.17.1.253 es.net. axfr
   ; (1 server found)

   ;; global options: printcmd

   es.net. 500 IN SOA siterequest.com.

   hostmaster.siterequest.com. 6 10800 3600 604800 60

   es.net. 500 IN NS siterequest.com.

   a.es.net. 30 IN A 192.17.1.100
```

```
b.es.net. 30 IN A 192.18.1.100

es.net. 500 IN SOA siterequest.com.

hostmaster.siterequest.com. 6 10800 3600 604800 60

;; Query time: 6 msec

;; SERVER: 192.17.1.253#53(192.17.1.253)

;; WHEN: Fri Mar 11 17:20:25 2011

;; XFR size: 5 records (messages 1, bytes 180)
```

About DNS views

A DNS *view* is a modification of a nameserver configuration based on the community attempting to access it. Using views, you can build multiple nameserver configurations on the same server, and have those configurations apply dynamically when the request originates from a specified source.

If your DNS handles requests from both inside and outside your company, you can create two views: internal and external.

Creating a DNS view

It is helpful to keep in mind that ZoneRunner™ contains a default view named: external.

Create an additional DNS view to modify the local nameserver configuration to allow a specific community to access it.

1. On the Main tab, click **DNS** > **Zones** > **ZoneRunner** > **View List**.
   The View List screen opens.
2. Click **Create**.
3. In the **View Name** field, type a name for the view.
4. From the **View Order** list, make a selection.

Option	Description
First	In the view hierarchy, this view is listed first.
Last	In the view hierarchy, this view is listed last.
After	In the view hierarchy, this view is listed immediately following the view that you select from the View List.

5. In the Options area, modify the match-clients statement based on your configuration.

View configuration type	Add to match-clients statement
Single view configuration	`view "external" { match-clients { "zrd-acl-000-000"; any; }; }`
Multiple view configuration, where you want to allow transfers from GTM	Modify the following match-clients statement to use the IP address of the GTM.

```
acl "internal-acl"
     { <IP address> ;
     };

view "internal" {
  match-clients {
    "zrd-acl-000-001";
    "internal-acl";
    <IP address> ;
  };

view "external" {
  match-clients {
    "zrd-acl-000-000";
    any;
  };
```

6. In the Options area, type additional configurations per your network design.
7. Click **Finished**.

Types of DNS zone files

This table describes the types of DNS zone files.

DNS file type	Description
Primary	Zone files for a primary zone contain, at minimum, the start of authority (SOA) and nameserver (NS) resource records for the zone. Primary zones are authoritative, that is, they respond to DNS queries for the domain or sub-domain. A zone can have only one SOA record, and must have at least one NS record.
Secondary	Zone files for a secondary zone are copies of the principal zone files. At an interval specified in the SOA record, secondary zones query the primary zone to check for and obtain updated zone data. A secondary zone responds authoritatively for the zone provided that the zone data is valid.
Stub	Stub zones are similar to secondary zones, except that stub zones contain only the NS records for the zone. Note that stub zones are a specific feature of the BIND implementation of DNS. F5 Networks recommends that you use stub zones only if you have a specific requirement for this functionality.
Forward	The zone file for a forwarding zone contains only information to forward DNS queries to another nameserver on a per-zone (or per-domain) basis.
Hint	The zone file for a hint zone specifies an initial set of root nameservers for the zone. Whenever the local nameserver starts, it queries a root nameserver in the hint zone file to obtain the most recent list of root nameservers. Zone file import.

Types of DNS resource records

This table describes the types of DNS resource records that ZoneRunner™ supports.

DNS file type	Description
SOA (Start of authority)	The start of authority resource record, SOA, starts every zone file and indicates that a nameserver is the best source of information for a particular zone. The SOA record indicates that a nameserver is authoritative for a zone. There must be exactly one SOA record per zone. Unlike other resource records, you create a SOA record only when you create a new master zone file.
A (Address)	The Address record, or A record, lists the IP address for a given host name. The name field is the host's name, and the address is the network interface address. There should be one A record for each IP address of the machine.
AAAA (IPv6 Address)	The IPv6 Address record, or AAAA record, lists the 128-bit IPv6 address for a given host name.
CNAME (Canonical Name)	The Canonical Name resource record, CNAME, specifies an alias or nickname for the official, or canonical, host name. This record must be the only one associated with the alias name. It is usually easier to supply one A record for a given address and use CNAME records to define alias host names for that address.
DNAME (Delegation of Reverse Name)	The Delegation of Reverse Name resource record, DNAME, specifies the reverse lookup of an IPv6 address. These records substitute the suffix of one domain name with another. The DNAME record instructs Global Traffic Manager™ (GTM™) (or any DNS server) to build an alias that substitutes a portion of the requested IP address with the data stored in the DNAME record.
HINFO (Host Information)	The Host Information resource record, HINFO, contains information on the hardware and operating system relevant to Global Traffic Manager (or other DNS).
MX (Mail Exchanger)	The Mail Exchange resource record, MX, defines the mail system(s) for a given domain.
NS (nameserver)	The nameserver resource record, NS, defines the nameservers for a given domain, creating a delegation point and a subzone. The first name field specifies the zone that is served by the nameserver that is specified in the nameservers name field. Every zone needs at least one nameserver.
PTR (Pointer)	A name pointer resource record, PTR, associates a host name with a given IP address. These records are used for reverse name lookups.
SRV (Service)	The Service resource record (SRV) is a pointer with which an alias for a given service is redirected to another domain. For example, if the fictional company Site Request has an FTP archive hosted on archive.siterequest.com, the IT department can create an SRV record with which the alias ftp.siterequest.com is redirected to archive.siterequest.com.
TXT (Text)	The Text resource record, TXT, allows you to supply any string of information, such as the location of a server or any other relevant information that you want available.

Chapter 11

Troubleshooting a BIG-IP System with a Rate-Limited License

About GTM and DNS rate-limited license statistics

If you have a BIG-IP® GTM™ or DNS Services rate-limited license, BIG-IP displays statistics about the rate limits including **Effective Rate Limit (RPS)**, **Object Count**, and **Rate Rejects**. Rate limit statistics are displayed separately for Global Traffic Management and DNS.

Viewing rate-limited license statistics

Ensure that the BIG-IP® system has a rate-limited license.

View statistics about GTM™ and DNS Services licensed service rates to help you determine when to upgrade your license.

1. On the Main tab, click **Statistics** > **Module Statistics** > **DNS** > **Delivery**.
   The DNS Delivery statistics screen opens.
2. From the **Statistics Type** list, select **Profiles**.
3. In the Global Profile Statistics area, in the Details column of the DNS profile, click **View**.
4. In the DNS area, view the **Effective Rate Limit (RPS)**, **Object Count**, and **Rate Rejects** statistics.

Statistic type	Description
Effective Rate Limit (RPS)	The number of DNS name resolution requests per second the BIG-IP system handles based on the rate-limited license installed on the system.
Object Count	The sum of these objects configured on the BIG-IP system: DNS Express™ zones, DNS cache resolvers, and DNSSEC zones.
Rate Rejects	The number of DNS requests that the BIG-IP system has rejected based on the rate limit of the license installed on the system.

5. In the Global Traffic Management area, view the **Effective Rate Limit (RPS)**, **Object Count**, and **Rate Rejects** statistics.

Statistic type	Description
Effective Rate Limit (RPS)	The number of DNS name resolution requests per second the GTM system handles based on the rate-limited license installed on the system.
Object Count	The sum of these objects configured on the GTM system: data centers, wide IPs, wide IP aliases, servers, GTM pools, GTM pool members, virtual servers, GTM iRules®, and topology records.
Rate Rejects	The number of DNS requests that the GTM system has rejected based on the rate limit of the license installed on the system. ***Tip:*** *The GTM license includes the DNS Services license. Global traffic management requests (requests for wide IPs) are a subset of DNS requests. Therefore, when the number of requests that GTM receives for a wide IP exceeds the DNS Services rate limit, the* ***Rate Rejects*** *count for DNS increments, rather than the* ***Rate Rejects*** *count for Global Traffic Management incrementing.*

Index

E

F

G

H

I

K

L

M

N

O

P

R

S

T

U

V

Z