BIG-IP® Global Traffic Manager™: Implementations

Version 11.5

Table of Contents

Legal Notices....9
Acknowledgments....11

Chapter 1: Integrating BIG-IP GTM Into a Network with BIG-IP LTM Systems....15
Overview: Integrating GTM with other BIG-IP systems on a network....16
About iQuery and communications between BIG-IP systems....16
Task summary....16
Defining a data center....16
Defining BIG-IP GTM systems....17
Defining BIG-IP LTM systems....18
Running the big3d_install script....19
Implementation result....20

Chapter 2: Integrating BIG-IP LTM Into a Network with BIG-IP GTM Systems....21
Overview: Integrating BIG-IP LTM with BIG-IP GTM systems....22
Defining a data center....22
Defining BIG-IP GTM systems....22
Defining BIG-IP LTM systems....24
Running the bigip_add script....25
Implementation result....25

Chapter 3: Adding a new BIG-IP GTM to a GTM Synchronization Group....27
Overview: Adding a BIG-IP GTM system to a GTM synchronization group....28
Enabling synchronization on the existing GTM....28
Creating a data center on the existing GTM....29
Defining a server on the existing GTM....29
Running the gtm_add script....30
Implementation result....31

Chapter 4: Delegating DNS Traffic to BIG-IP GTM....33
Overview: Delegating DNS traffic to wide IPs on BIG-IP GTM....34
About listeners....34
Task summary....34
Creating a delegated zone on a local DNS server....35
Creating listeners to handle traffic for wide IPs....35
Implementation result....36

Chapter 5: Redirecting DNS Queries Using a CNAME Record....37
Overview: Redirecting DNS queries using a CNAME record 38

About CNAME records....38
Task summary....38
Creating a pool using a CNAME....38
Creating a wide IP with a CNAME pool....39
Viewing statistics for wide IP CNAME resolutions....39
Implementation result....39

Chapter 6: Replacing a DNS Server with BIG-IP GTM....41
Overview: Replacing a DNS server with BIG-IP GTM....42
About listeners....42
Task summary....42
Configuring BIND servers to allow zone transfers....43
Performing zone transfers from the legacy DNS server....43
Creating a self IP address using the IP address of the legacy DNS server....44
Designating GTM as the primary server for the zone....44
Creating listeners to alert GTM to DNS traffic destined for the system....45
Creating a wide IP....45
Implementation result....46

Chapter 7: Placing BIG-IP GTM in Front of a DNS Server....47
Overview: Configuring GTM to screen traffic to an existing DNS server....48
About listeners....48
About wildcard listeners....48
Task summary....49
Placing BIG-IP GTM on your network to forward traffic....49
Creating listeners to forward traffic to a DNS server....49
Creating a wide IP....50
Implementation result....50

Chapter 8: Placing BIG-IP GTM in front of a Pool of DNS Servers....51
Overview: Screening and forwarding non-wide IP traffic to a pool of DNS servers....52
About listeners....52
Task summary....52
Creating a pool of local DNS servers....53
Creating listeners that alert GTM to DNS queries for a pool of DNS servers....53
Implementation result....54

Chapter 9: Configuring GTM to Determine PGW Health and Availability....55
Overview: Configuring GTM to determine packet gateway health and availability....56
Defining a data center....57
Defining BIG-IP GTM systems....57
Defining packet gateway systems....58
Creating listeners to identify DNS traffic for an APN....59

Creating a custom GTP monitor....60
Creating a pool of packet gateway systems....61
Configuring a wide IP for load balancing APN lookups....61

Chapter 10: Configuring GTM on a Network with One Route Domain....63
Overview: How do I deploy BIG-IP GTM on a network with one route domain?....64
Creating VLANs for a route domain on BIG-IP LTM....65
Creating a route domain on the BIG-IP system....65
Creating a self IP address for a route domain on BIG-IP LTM....66
Defining a server for a route domain on BIG-IP GTM....66
Implementation result....67

Chapter 11: Configuring GTM on a Network with Multiple Route Domains....69
Overview: How do I deploy BIG-IP GTM on a network with multiple route domains?....70
Creating VLANs for a route domain on BIG-IP LTM....72
Creating a route domain on BIG-IP LTM....72
Creating a self IP address for a route domain on BIG-IP LTM....73
Disabling auto-discovery at the global-level on BIG-IP GTM....73
Defining a server for a route domain on BIG-IP GTM....73
Implementation result....74

Chapter 12: Setting Up a BIG-IP GTM Redundant System Configuration....75
Overview: Configuring a BIG-IP GTM redundant system....76
Defining an NTP server....76
Creating listeners to identify DNS traffic....76
Defining a data center....77
Defining a server to represent each BIG-IP system 77
Enabling global traffic configuration synchronization....78
Running the gtm_add script 79

Chapter 13: Authenticating with SSL Certificates Signed by a Third Party....81
Overview: Authenticating with SSL certificates signed by a third party....82
About SSL authentication levels....82
Configuring Level 1 SSL authentication....82
Importing the device certificate....82
Importing the root certificate for the gtmd agent....83
Importing the root certificate for the big3d agent....83
Verifying the certificate exchange....83
Implementation Results....84
Configuring certificate chain SSL authentication....84
Creating a certificate chain file 84
Importing the device certificate from the last CA server in the chain....84
Importing a certificate chain file for the gtmd agent....85

Importing a certificate chain for the big3d agent....85
Verifying the certificate chain exchange....85
Implementation result....86

Chapter 14: Configuring a TTL in a DNS NoError Response....87
Overview: Configuring a TTL in an IPv6 DNS NoError Response....88
About SOA records and negative caching....88
Task summary....88
Creating a pool....88
Creating a wide IP that provides for negative caching 89
Implementation result....89

Chapter 15: Configuring Device-Specific Probing and Statistics Collection....91
Overview: Configuring device-specific probing and statistics collection....92
About Prober pools....92
About Prober pool status....93
About Prober pool statistics....93
Task summary....93
Defining a data center....94
Defining a server....94
Creating a Prober pool....95
Assigning a Prober pool to a data center....96
Assigning a Prober pool to a server....96
Viewing Prober pool statistics and status....96
Determining which Prober pool member marked a resource down....97
Implementation result....97

Chapter 16: Configuring How and When GTM Saves Configuration Changes....99
Overview: Configuring how and when GTM saves configuration changes....100
Changing the automatic configuration save timeout....100
Enabling manual saves of configuration changes....100
Configuring how and when GTM saves configuration changes using tmsh....101

Chapter 17: Configuring Logging of Global Server Load Balancing Decisions....103
About logging global server load-balancing decisions....104
Configuring logs for global server load-balancing decisions 104

Chapter 18: Monitoring Third-Party Servers with SNMP....105
Overview: SNMP monitoring of third-party servers....106
Creating an SNMP monitor....106
Defining a third-party host server that is running SNMP....106
Implementation result....107

Chapter 19: Troubleshooting a BIG-IP System with a Rate-Limited License.....109
About GTM and DNS rate-limited license statistics.....110
Viewing rate-limited license statistics.....110

Chapter 20: How to Diagnose Network Connection Issues.....111
Diagnosing network connection issues.....112
Viewing iQuery statistics 112
iQuery statistics descriptions.....112

Legal Notices

Publication Date

This document was published on February 21, 2014.

Publication Number

MAN-0388-04

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 Gabriel Forté.

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 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 unbound software from NLnetLabs. Copyright ©2007. 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

Chapter 1

Integrating BIG-IP GTM Into a Network with BIG-IP LTM Systems

- *Overview: Integrating GTM with other BIG-IP systems on a network*
- *Task summary*
- *Implementation result*

Overview: Integrating GTM with other BIG-IP systems on a network

You can add BIG-IP® Global Traffic Manager™ (GTM™) systems to a network in which BIG-IP® Local Traffic Manager™ (LTM®) systems and BIG-IP Link Controller™ systems are already present. This expands your load balancing and traffic management capabilities beyond the local area network. For this implementation to be successful, you must authorize communications between the systems.

Note: *The GTM devices in a GTM synchronization group, and the LTM and Link Controller™ devices that are configured to communicate with the devices in the GTM synchronization group must have TCP port 4353 open through the firewall between the systems. The BIG-IP devices connect and communicate through this port.*

About iQuery and communications between BIG-IP systems

The `gtmd` agent on BIG-IP® Global Traffic Manager™ (GTM™) uses the iQuery® protocol to communicate with the local `big3d` agent, and the `big3d` agents installed on other BIG-IP systems. The `gtmd` agent monitors both the availability of the BIG-IP systems, and the integrity of the network paths between the systems that host a domain and the local DNS servers that attempt to connect to that domain.

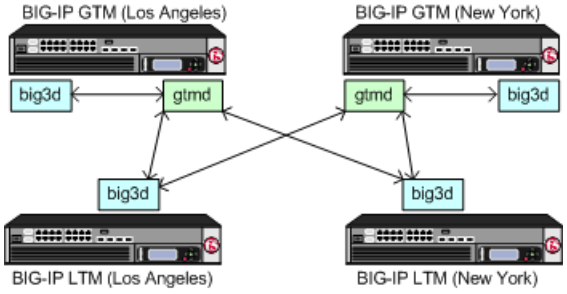

Figure 1: Communications between big3d and gtmd agents using iQuery

Task summary

To authorize communications between BIG-IP® systems, perform the following tasks on the BIG-IP GTM™ system that you are adding to the network.

Defining a data center
Defining BIG-IP GTM systems
Defining BIG-IP LTM systems
Running the big3d_install script

Defining a data center

On BIG-IP®GTM™, create a data center to contain the servers that reside on a subnet of your network.

1. On the Main tab, click **DNS** > **GSLB** > **Data Centers**.

The Data Center List screen opens.

2. Click **Create**.
   The New Data Center screen opens.
3. In the **Name** field, type a name to identify the data center.

   Important: *The data center name is limited to 63 characters.*

4. In the **Location** field, type the geographic location of the data center.
5. In the **Contact** field, type the name of either the administrator or the department that manages the data center.
6. From the **State** list, select **Enabled**.
7. Click **Finished**.

Now you can create server objects and assign them to this data center.

Repeat these steps to create additional data centers.

Defining BIG-IP GTM systems

Ensure that at least one data center exists in the configuration before you start creating a server.

On BIG-IP® GTM™, create a server object to represent the GTM system itself.

1. On the Main tab, click **DNS** > **GSLB** > **Servers**.
   The Server List screen opens.
2. Click **Create**.
   The New Server screen opens.
3. In the **Name** field, type a name for the server.

   Important: *Server names are limited to 63 characters.*

4. From the **Product** list, select **BIG-IP System (Single)**.
   The server type determines the metrics that the system can collect from the server.
5. In the Address List area, add the IP addresses of the server.
   You can add more than one IP address, depending on how the server interacts with the rest of your network.

   Important: *You must use a self IP address for a BIG-IP system; you cannot use the management IP address.*

6. From the **Data Center** list, select the data center where the server resides.
7. In the Health Monitors area, assign the **bigip** monitor to the server by moving it from the **Available** list to the **Selected** list.
8. From the **Virtual Server Discovery** list, select how you want virtual servers to be added to the system.

Option	Description
Disabled	The system does not use the discovery feature to automatically add virtual servers. This is the default value. Use this option for a standalone GTM system or for a GTM/LTM® combo system when you plan to manually add virtual servers to the system, or if your network uses multiple route domains.

Option	Description
Enabled	The system uses the discovery feature to automatically add virtual servers. Use this option for a GTM/LTM combo system when you want the GTM system to discover LTM virtual servers.
Enabled (No Delete)	The system uses the discovery feature to automatically add virtual servers and does not delete any virtual servers that already exist. Use this option for a GTM/LTM combo system when you want the GTM system to discover LTM virtual servers.

9. In the Virtual Server List area, if you selected **Disabled** from the **Virtual Server Discovery** list, specify the virtual servers that are resources on this server.
   a) In the **Name** field, type the name of the virtual server.
   b) In the **Address** field, type the IP address of the virtual server.
   c) From the **Service Port** list, select the port the server uses.
   d) Click **Add**.

10. From the **Link Discovery** list, select how you want links to be added to the system.

Option	Description
Disabled	The system does not use the discovery feature to automatically add links. This is the default value. Use this option for a standalone GTM system or for a GTM/LTM combo system when you plan to manually add links to the system.
Enabled	The system uses the discovery feature to automatically add links. Use this option for a GTM/LTM combo system when you want BIG-IP GTM to discover links.
Enabled (No Delete)	The system uses the discovery feature to automatically add links and does not delete any links that already exist. Use this option for a GTM/LTM combo system when you want GTM to discover links.

11. Click **Create**.
    The Server List screen opens displaying the new server in the list.

Defining BIG-IP LTM systems

On GTM™, define servers that represent the LTM® systems in your network.

1. On the Main tab, click **DNS** > **GSLB** > **Servers**.
   The Server List screen opens.
2. Click **Create**.
   The New Server screen opens.
3. In the **Name** field, type a name for the server.

   Important: *Server names are limited to 63 characters.*

4. From the **Product** list, select either **BIG-IP System (Single)** or **BIG-IP System (Redundant)**.
   The server type determines the metrics that the system can collect from the server.
5. In the Address List area, add the IP addresses of the server.
   You can add more than one IP address, depending on how the server interacts with the rest of your network.

Important: *You must use a self IP address for a BIG-IP system; you cannot use the management IP address.*

6. From the **Data Center** list, select the data center where the server resides.
7. In the Health Monitors area, assign the **bigip** monitor to the server by moving it from the **Available** list to the **Selected** list.
8. From the **Virtual Server Discovery** list, select how you want virtual servers to be added to the system.

Option	Description
Disabled	The system does not use the discovery feature to automatically add virtual servers. This is the default value. Use this option for a standalone GTM system or for a GTM/LTM® combo system when you plan to manually add virtual servers to the system, or if your network uses multiple route domains.
Enabled	The system uses the discovery feature to automatically add virtual servers. Use this option for a GTM/LTM combo system when you want the GTM system to discover LTM virtual servers.
Enabled (No Delete)	The system uses the discovery feature to automatically add virtual servers and does not delete any virtual servers that already exist. Use this option for a GTM/LTM combo system when you want the GTM system to discover LTM virtual servers.

9. In the Virtual Server List area, if you selected **Disabled** from the **Virtual Server Discovery** list, specify the virtual servers that are resources on this server.
   a) In the **Name** field, type the name of the virtual server.
   b) In the **Address** field, type the IP address of the virtual server.
   c) From the **Service Port** list, select the port the server uses.
   d) Click **Add**.
10. From the **Link Discovery** list, select how you want links to be added to the system.

Option	Description
Disabled	The system does not use the discovery feature to automatically add links. This is the default value. Use this option for a standalone GTM system or for a GTM/LTM combo system when you plan to manually add links to the system.
Enabled	The system uses the discovery feature to automatically add links. Use this option for a GTM/LTM combo system when you want BIG-IP GTM to discover links.
Enabled (No Delete)	The system uses the discovery feature to automatically add links and does not delete any links that already exist. Use this option for a GTM/LTM combo system when you want GTM to discover links.

11. Click **Create**.
    The Server List screen opens displaying the new server in the list.

Running the big3d_install script

Determine the self IP addresses of the BIG-IP® systems that you want to upgrade with the latest `big3d` agent. Ensure that port `22` is open on these systems.

Run the `big3d_install` script on the GTM™ system you are adding to your network. This upgrades the `big3d` agents on the other BIG-IP systems on your network. It also instructs these systems to authenticate

with the other BIG-IP systems through the exchange of SSL certificates. For additional information about running the script, see SOL8195 on AskF5.com (`www.askf5.com`).

Note: *You must perform this task from the command-line interface.*

Important: *All target BIG-IP systems must be running the same or an older version of BIG-IP software.*

1. Log in as `root` to the BIG-IP GTM system you are adding to your network.
2. Run this command to access `tmsh`:

   ```
   tmsh
   ```

3. Run this command to run the `big3d_install` script:

   ```
   run gtm big3d_install <IP_addresses_of_target BIG-IP_systems>
   ```

   The script instructs GTM to connect to each specified BIG-IP system.
4. If prompted, enter the `root` password for each system.

The SSL certificates are exchanged, authorizing communications between the systems. The `big3d` agent on each system is upgraded to the same version as is installed on the GTM system from which you ran the script.

Implementation result

You now have an implementation in which the BIG-IP® systems can communicate with each other. GTM™ can now use the other BIG-IP systems when load balancing DNS queries, and can acquire statistics and status information for the virtual servers these systems manage.

Chapter 2

Integrating BIG-IP LTM Into a Network with BIG-IP GTM Systems

- *Overview: Integrating BIG-IP LTM with BIG-IP GTM systems*
- *Implementation result*

Overview: Integrating BIG-IP LTM with BIG-IP GTM systems

You can add BIG-IP® Local Traffic Manager™ (LTM™) systems to a network in which BIG-IP® Global Traffic Manager™ (GTM™) systems are already present. This expands your load balancing and traffic management capabilities to include the local area network. For this implementation to be successful, you must authorize communications between the LTM and GTM systems. When the LTM and GTM systems use the same version of the `big3d agent`, you run the `bigip_add` utility to authorize communications between the systems.

Note: *The BIG-IP GTM and BIG-IP LTM systems must have TCP port 4353 open through the firewall between the systems. The BIG-IP systems connect and communicate through this port.*

Task summary

To authorize communications between BIG-IP® GTM and BIG-IP LTM systems, perform the following tasks on GTM.

Defining a data center
Defining BIG-IP GTM systems
Defining BIG-IP LTM systems
Running the bigip_add script

Defining a data center

On BIG-IP®GTM™, create a data center to contain the servers that reside on a subnet of your network.

1. On the Main tab, click **DNS** > **GSLB** > **Data Centers**.
   The Data Center List screen opens.
2. Click **Create**.
   The New Data Center screen opens.
3. In the **Name** field, type a name to identify the data center.

   Important: *The data center name is limited to 63 characters.*
4. In the **Location** field, type the geographic location of the data center.
5. In the **Contact** field, type the name of either the administrator or the department that manages the data center.
6. From the **State** list, select **Enabled**.
7. Click **Finished**.

Now you can create server objects and assign them to this data center.

Repeat these steps to create additional data centers.

Defining BIG-IP GTM systems

Ensure that at least one data center exists in the configuration before you start creating a server.

On BIG-IP® GTM™, create a server object to represent the GTM system itself.

1. On the Main tab, click **DNS** > **GSLB** > **Servers**.
   The Server List screen opens.
2. Click **Create**.
   The New Server screen opens.
3. In the **Name** field, type a name for the server.

   Important: *Server names are limited to 63 characters.*

4. From the **Product** list, select **BIG-IP System (Single)**.
   The server type determines the metrics that the system can collect from the server.
5. In the Address List area, add the IP addresses of the server.
   You can add more than one IP address, depending on how the server interacts with the rest of your network.

   Important: *You must use a self IP address for a BIG-IP system; you cannot use the management IP address.*

6. From the **Data Center** list, select the data center where the server resides.
7. In the Health Monitors area, assign the **bigip** monitor to the server by moving it from the **Available** list to the **Selected** list.
8. From the **Virtual Server Discovery** list, select how you want virtual servers to be added to the system.

Option	Description
Disabled	The system does not use the discovery feature to automatically add virtual servers. This is the default value. Use this option for a standalone GTM system or for a GTM/LTM® combo system when you plan to manually add virtual servers to the system, or if your network uses multiple route domains.
Enabled	The system uses the discovery feature to automatically add virtual servers. Use this option for a GTM/LTM combo system when you want the GTM system to discover LTM virtual servers.
Enabled (No Delete)	The system uses the discovery feature to automatically add virtual servers and does not delete any virtual servers that already exist. Use this option for a GTM/LTM combo system when you want the GTM system to discover LTM virtual servers.

9. In the Virtual Server List area, if you selected **Disabled** from the **Virtual Server Discovery** list, specify the virtual servers that are resources on this server.
   a) In the **Name** field, type the name of the virtual server.
   b) In the **Address** field, type the IP address of the virtual server.
   c) From the **Service Port** list, select the port the server uses.
   d) Click **Add**.
10. From the **Link Discovery** list, select how you want links to be added to the system.

Option	Description
Disabled	The system does not use the discovery feature to automatically add links. This is the default value. Use this option for a standalone GTM system or for a GTM/LTM combo system when you plan to manually add links to the system.
Enabled	The system uses the discovery feature to automatically add links. Use this option for a GTM/LTM combo system when you want BIG-IP GTM to discover links.

Option	Description
Enabled (No Delete)	The system uses the discovery feature to automatically add links and does not delete any links that already exist. Use this option for a GTM/LTM combo system when you want GTM to discover links.

11. Click **Create**.
The Server List screen opens displaying the new server in the list.

Defining BIG-IP LTM systems

On GTM™, define servers that represent the LTM® systems in your network.

1. On the Main tab, click **DNS** > **GSLB** > **Servers**.
The Server List screen opens.
2. Click **Create**.
The New Server screen opens.
3. In the **Name** field, type a name for the server.

Important: *Server names are limited to 63 characters.*

4. From the **Product** list, select either **BIG-IP System (Single)** or **BIG-IP System (Redundant)**.
The server type determines the metrics that the system can collect from the server.
5. In the Address List area, add the IP addresses of the server.
You can add more than one IP address, depending on how the server interacts with the rest of your network.

Important: *You must use a self IP address for a BIG-IP system; you cannot use the management IP address.*

6. From the **Data Center** list, select the data center where the server resides.
7. In the Health Monitors area, assign the **bigip** monitor to the server by moving it from the **Available** list to the **Selected** list.
8. From the **Virtual Server Discovery** list, select how you want virtual servers to be added to the system.

Option	Description
Disabled	The system does not use the discovery feature to automatically add virtual servers. This is the default value. Use this option for a standalone GTM system or for a GTM/LTM® combo system when you plan to manually add virtual servers to the system, or if your network uses multiple route domains.
Enabled	The system uses the discovery feature to automatically add virtual servers. Use this option for a GTM/LTM combo system when you want the GTM system to discover LTM virtual servers.
Enabled (No Delete)	The system uses the discovery feature to automatically add virtual servers and does not delete any virtual servers that already exist. Use this option for a GTM/LTM combo system when you want the GTM system to discover LTM virtual servers.

9. In the Virtual Server List area, if you selected **Disabled** from the **Virtual Server Discovery** list, specify the virtual servers that are resources on this server.

a) In the **Name** field, type the name of the virtual server.
b) In the **Address** field, type the IP address of the virtual server.
c) From the **Service Port** list, select the port the server uses.
d) Click **Add**.

10. From the **Link Discovery** list, select how you want links to be added to the system.

Option	Description
Disabled	The system does not use the discovery feature to automatically add links. This is the default value. Use this option for a standalone GTM system or for a GTM/LTM combo system when you plan to manually add links to the system.
Enabled	The system uses the discovery feature to automatically add links. Use this option for a GTM/LTM combo system when you want BIG-IP GTM to discover links.
Enabled (No Delete)	The system uses the discovery feature to automatically add links and does not delete any links that already exist. Use this option for a GTM/LTM combo system when you want GTM to discover links.

11. Click **Create**.
The Server List screen opens displaying the new server in the list.

Running the bigip_add script

Determine the self IP addresses of the LTM® systems that you want to communicate with GTM™.

Run the `bigip_add` script on the GTM system you are installing on a network that includes other BIG-IP® systems of the same version. This script exchanges SSL certificates so that each system is authorized to communicate with the other.

Note: *You must perform this task from the command-line interface.*

1. Log in as `root` to the GTM system you are installing on your network.
2. Run this command to access `tmsh`.

```
tmsh
```

3. Run this command to run the `bigip_add` utility:

```
run gtm bigip_add <IP_addresses_of_BIG-IP_LTM_systems>
```

The utility exchanges SSL certificates so that each system is authorized to communicate with the other.

The specified BIG-IP systems can now communicate with GTM.

Implementation result

You now have an implementation in which the BIG-IP® systems can communicate with each other. BIG-IP GTM™ can now use the other BIG-IP systems when load balancing DNS queries, and can acquire statistics and status information for the virtual servers the other BIG-IP systems manage.

Chapter 3

Adding a new BIG-IP GTM to a GTM Synchronization Group

- *Overview: Adding a BIG-IP GTM system to a GTM synchronization group*
- *Implementation result*

Overview: Adding a BIG-IP GTM system to a GTM synchronization group

You can configure BIG-IP® Global Traffic Manager™ (GTM)™ systems in collections called GTM synchronization groups. All BIG-IP GTM systems in the same *GTM synchronization group* have the same rank, exchange heartbeat messages, and share probing responsibility.

Configuration changes to one device in a GTM synchronization group are synchronized incrementally across the devices in the group. That is, only the data that has changed on a GTM device is synchronized to the other devices in the group. Although incremental synchronization is the default behavior, if an incremental synchronization fails, the system automatically performs a full configuration synchronization.

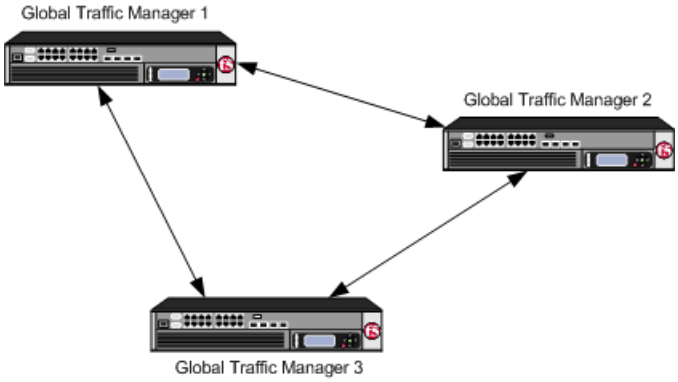

Figure 2: BIG-IP GTM systems in a GTM synchronization group

When you add a BIG-IP® (GTM)™ system to a network that contains older BIG-IP GTM systems, the devices can exchange heartbeat messages, even though the BIG-IP software versions are different. However, to add a GTM to a configuration synchronization group, you must run the `gtm_add` script.

Task Summary

When adding a BIG-IP® GTM to a network that already contains BIG-IP GTM systems in a synchronization group, perform the following tasks.

Enabling synchronization on the existing GTM
Creating a data center on the existing GTM
Defining a server on the existing GTM
Running the gtm_add script

Enabling synchronization on the existing GTM

Ensure that BIG-IP® GTM™ references your NTP servers.

Decide to which GTM synchronization group you want to add the GTM system. Make certain that at least one previously-configured GTM belongs to that GTM synchronization group.

Enable synchronization on the system to ensure that the GTM system that is already installed on your network can share configuration changes with other GTM systems that you add to the GTM synchronization group.

1. On the Main tab, click **DNS** > **Settings** > **GSLB** > **General**.
   The General configuration screen opens.
2. Select the **Synchronize** check box.

3. In the **Group Name** field, type the name of the synchronization group to which you want this system to belong.
4. In the **Time Tolerance** field, type the maximum number of seconds allowed between the time settings on this system and the other systems in the synchronization group.

   The lower the value, the more often this system makes a log entry indicating that there is a difference.

   Tip: *If you are using NTP, leave this setting at the default value of* `10`*. In the event that NTP fails, the system uses the time_tolerance variable to maintain synchronization.*
5. Click **Update**.

When a change is made on one GTM system in the GTM synchronization group, that change is automatically synchronized to the other systems in the group.

Creating a data center on the existing GTM

Create a data center on the existing GTM™ system to represent the location where the new GTM system resides.

1. On the Main tab, click **DNS** > **GSLB** > **Data Centers**.
   The Data Center List screen opens.
2. Click **Create**.
   The New Data Center screen opens.
3. In the **Name** field, type a name to identify the data center.

   Important: *The data center name is limited to 63 characters.*
4. In the **Location** field, type the geographic location of the data center.
5. In the **Contact** field, type the name of either the administrator or the department that manages the data center.
6. From the **State** list, select **Enabled** or **Disabled**.

   The default is **Enabled**, which specifies that the data center and its resources are available for load balancing.
7. Click **Finished**.

Defining a server on the existing GTM

Ensure that a data center where the new GTM™ system resides is available in the configuration of the existing GTM.

Define a new server, on the existing GTM system, to represent the new GTM system.

1. On the Main tab, click **DNS** > **GSLB** > **Servers**.
   The Server List screen opens.
2. Click **Create**.
   The New Server screen opens.
3. In the **Name** field, type a name for the server.

   Important: *Server names are limited to 63 characters.*

4. From the **Product** list, select **BIG-IP System (Single)**.
   The server type determines the metrics that the system can collect from the server.
5. In the Address List area, add the IP address of the server.

   Important: *You must use a self IP address for a BIG-IP® system; you cannot use the management IP address.*

6. From the **Data Center** list, select the data center where the server resides.
7. From the **Virtual Server Discovery** list, select how you want virtual servers to be added to the system.

Option	Description
Disabled	The system does not use the discovery feature to automatically add virtual servers. This is the default value. Use this option for a standalone GTM system or for a GTM/LTM® combo system when you plan to manually add virtual servers to the system, or if your network uses multiple route domains.
Enabled	The system uses the discovery feature to automatically add virtual servers. Use this option for a GTM/LTM combo system when you want the GTM system to discover LTM virtual servers.
Enabled (No Delete)	The system uses the discovery feature to automatically add virtual servers and does not delete any virtual servers that already exist. Use this option for a GTM/LTM combo system when you want the GTM system to discover LTM virtual servers.

8. In the Virtual Server List area, if you selected **Disabled** from the **Virtual Server Discovery** list, specify the virtual servers that are resources on this server.
   a) In the **Name** field, type the name of the virtual server.
   b) In the **Address** field, type the IP address of the virtual server.
   c) From the **Service Port** list, select the port the server uses.
   d) Click **Add**.
9. Click **Create**.
   The Server List screen opens displaying the new server in the list.

The status of the newly defined GTM system is Unknown, because you have not yet run the `gtm_add` script.

Running the gtm_add script

Determine the self IP address of a GTM™ system in the GTM synchronization group to which you want to add another GTM.

Run the `gtm_add` script on the GTM system you are adding to your network to acquire the configuration settings from a GTM system that is already installed on your network.

Note: *You must perform this task from the command-line interface.*

1. Log in as `root` to the GTM system you are adding to your network.
2. Run this command to access `tmsh`.

   ```
   tmsh
   ```

3. Run this command to run the `gtm_add` script

   ```
   run gtm gtm_add
   ```

a) Press the `y` key to start the `gtm_add` script.
b) Type the IP address of the GTM system in the synchronization group to which you are adding this GTM system.
c) Press `Enter`.
d) If prompted, type the `root` password.
e) Press `Enter`.

The GTM system you are installing on your network acquires the configuration of the GTM system already installed on your network.

Implementation result

The new BIG-IP® GTM™ system that you added to the network is a part of a GTM synchronization group. Changes you make to any system in the GTM synchronization group are automatically propagated to all other GTM systems in the group.

Chapter 4

Delegating DNS Traffic to BIG-IP GTM

- *Overview: Delegating DNS traffic to wide IPs on BIG-IP GTM*
- *Task summary*
- *Implementation result*

Overview: Delegating DNS traffic to wide IPs on BIG-IP GTM

BIG-IP® Global Traffic Manager™ (GTM™) resolves DNS queries that match a wide IP name. BIG-IP GTM can work in conjunction with an existing DNS server on your network. In this situation, you configure the DNS server to delegate wide IP-related requests to BIG-IP GTM for name resolution.

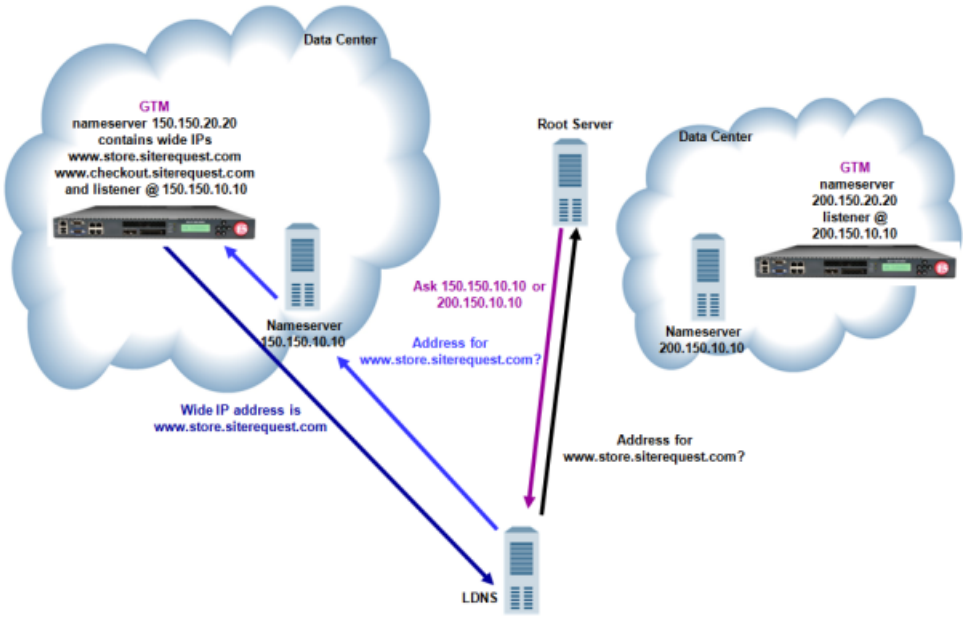

Figure 3: Traffic flow when DNS server delegates traffic to BIG-IP GTM

This implementation focuses on the fictional company SiteRequest that recently purchased BIG-IP GTM to help resolve queries for two web-based applications: `store.siterequest.com` and `checkout.siterequest.com`. These applications are delegated zones of `www.siterequest.com`. Currently, a DNS server manages `www.siterequest.com`.

SiteRequest administrators have already configured BIG-IP GTM with two wide IPs, `www.store.siterequest.com` and `www.checkout.siterequest.com`. These wide IPs correspond to the two web applications.

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 query is sent to the IP address of the listener, BIG-IP GTM™ either handles the request locally or forwards the request to the appropriate resource.

Task summary

Perform these tasks to delegate DNS traffic to wide IPs on BIG-IP GTM™.

Creating a delegated zone on a local DNS server
Creating listeners to handle traffic for wide IPs

Creating a delegated zone on a local DNS server

Determine which DNS servers will delegate wide IP-related requests to BIG-IP® GTM™.

If you are using BIND servers and you are unfamiliar with how to modify the files on these servers, consider reviewing the fifth edition of *DNS and BIND*, available from O'Reilly Media.

In order for GTM to manage the web applications of `store.siterequest.com` and `checkout.siterequest.com`, you must create a delegated zone on the DNS server that manages `www.siterequest.com`. Perform the following steps on the selected DNS server.

1. Create an *address record* (A record) that defines the domain name and IP address of each GTM in your network.
2. Create a *nameserver record* (NS record) that defines the delegated zone for which GTM is responsible.
3. Create *canonical name* records (CNAME records) to forward requests for `store.siterequest.com` and `checkout.siterequest.com` to the wide IPs `store.siterequest.com` and `checkout.siterequest.com`, respectively.

Creating listeners to handle traffic for wide IPs

Determine the self IP address on which you want BIG-IP® GTM™ to listen for DNS queries for the wide IPs configured on the system.

Create listeners that identify the wide IP traffic for which GTM™ is responsible. Create four listeners: two that use the UDP protocol (one each for an IPv4 address and IPv6 address), and two that use the TCP protocol (one each for an IPv4 address and IPv6 address).

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

---

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.

   The destination is a self IP address on GTM.
5. From the **VLAN Traffic** list, select **All VLANs**.
6. In the Service area, from the **Protocol** list, select **UDP**.
7. Click **Repeat**.

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.

Implementation result

You now have an implementation of BIG-IP® GTM™ in which the DNS server manages DNS traffic unless the query is for `store.sitrequest.com` or `checkout.siterequest.com`. When the DNS server receives these queries, it delegates them to BIG-IP GTM, which then load balances the queries to the appropriate wide IPs.

Chapter 5

Redirecting DNS Queries Using a CNAME Record

- *Overview: Redirecting DNS queries using a CNAME record*
- *Task summary*
- *Implementation result*

Overview: Redirecting DNS queries using a CNAME record

When you want to redirect DNS queries for a web site to a different web site, create a wide IP that represents the original web site, and add a pool configured with a CNAME to the wide IP to redirect the requests to the new destination.

The executives at `siterequest.com` recently purchased a competitor. Site Request's administrator wants to redirect DNS queries for `competitor.com` to a rebranded web site named `competitor.siterequest.com`.

About CNAME records

A *CNAME* record specifies that a domain name is an alias of another domain. When you create a pool with a canonical name, BIG-IP® Global Traffic Manager™ (GTM™) responds to DNS name resolution requests for the CNAME with the real fully qualified domain name (FQDN).

Task summary

Perform these tasks to redirect a DNS request using a wide IP, which includes a pool that is configured with a CNAME.

Creating a pool using a CNAME
Creating a wide IP with a CNAME pool
Viewing statistics for wide IP CNAME resolutions

Creating a pool using a CNAME

Create a pool to which the system can load balance DNS queries using a CNAME record, rather than pool members. For example, you can name the pool `competitor_redirect` and use a CNAME of `competitor.siterequest.com`.

1. On the Main tab, click **DNS** > **GSLB** > **Pools**.
   The Pools list screen opens.
2. Click **Create**.
3. In the **Name** field, type a name for the pool.
   Names must begin with a letter, and can contain only letters, numbers, and the underscore (_) character.

   Important: *The pool name is limited to 63 characters.*

4. From the **Configuration** list, select **Advanced**.
5. In the **CNAME** field, type the canonical name of the zone to which you want GTM™ to send DNS queries.

Tip: When you provide a canonical name, you do not add members to the pool, because the CNAME record always takes precedence over pool members. Additionally, a pool with a CNAME is not monitored for availability.

6. Click **Finished**.

Creating a wide IP with a CNAME pool

Ensure that a pool configured with a CNAME exists in the BIG-IP® configuration.

Create a wide IP that includes a pool configured with a CNAME to redirect DNS queries for a web site, to a different web site.

1. On the Main tab, click **DNS** > **GSLB** > **Wide IPs**.
   The Wide IP List screen opens.
2. Click **Create**.
   The New Wide IP screen opens.
3. In the **Name** field, type a name for the wide IP.

Tip: You can use two different wildcard characters in the wide IP name: asterisk (*) to represent several characters and question mark (?) to represent a single character. This reduces the number of aliases you have to add to the configuration.

4. From the **Pool** list, select the CNAME pool, and then click **Add**.
5. Click **Finished**.

Viewing statistics for wide IP CNAME resolutions

Ensure that a wide IP that includes a pool configured with a CNAME exists in the BIG-IP® configuration.

You can view the number of DNS queries that GTM™ resolved using a CNAME record.

1. On the Main tab, click **Statistics** > **Module Statistics** > **DNS** > **GSLB**.
   The Global Traffic statistics screen opens.
2. From the **Statistics Type** list, select **Wide IPs**.
   Information displays about the cumulative number of DNS name resolution requests processed by the wide IP, and the number of requests load balanced using specific methods.

Implementation result

You now have an implementation in which BIG-IP® GTM™ resolves a DNS query for a wide IP to a CNAME. The LDNS must further resolve the CNAME to an IP address.

Chapter 6

Replacing a DNS Server with BIG-IP GTM

- *Overview: Replacing a DNS server with BIG-IP GTM*
- *Task summary*
- *Implementation result*

Overview: Replacing a DNS server with BIG-IP GTM

BIG-IP® Global Traffic Manager™ (GTM™) load balances incoming wide IP traffic to your network resources. BIG-IP GTM can also replace a local DNS server as the authoritative nameserver for wide IPs, zones, and all other DNS-related traffic. You can configure BIG-IP GTM to replace the DNS server that currently manages `www.siterequest.com`. BIG-IP GTM becomes the authoritative nameserver for `www.siterequest.com` and load balances traffic across the web-based applications `store.siterequest.com` and `checkout.siterequest.com`.

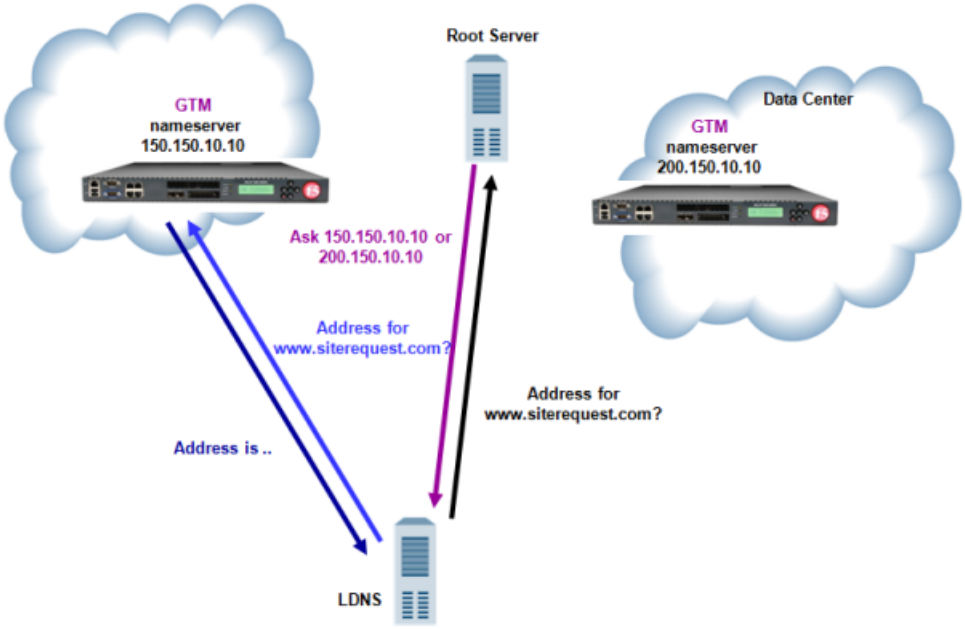

Figure 4: Traffic flow when BIG-IP GTM replaces DNS server

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 query is sent to the IP address of the listener, BIG-IP GTM™ either handles the request locally or forwards the request to the appropriate resource.

Task summary

Perform these tasks to replace a DNS server with BIG-IP GTM.

Configuring BIND servers to allow zone transfers
Performing zone transfers from the legacy DNS server
Creating a self IP address using the IP address of the legacy DNS server
Designating GTM as the primary server for the zone
Creating listeners to alert GTM to DNS traffic destined for the system
Creating a wide IP

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 ; };
```

Performing zone transfers from the legacy DNS server

Ensure that you have configured the legacy DNS server with an allow-transfer statement that authorizes zone transfers to BIG-IP® GTM™.

In order for GTM to perform a zone transfer from the legacy DNS server, create a new zone.

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 the view that you want this zone to be a member of.
   The default view is **external**.
4. In the **Zone Name** field, type a name for the zone file in this format, including the trailing dot: `db.[viewname].[zonename].`
   For example, `db.external.siterequest.com.`
5. From the **Zone Type** list, select **Master**.
6. From the **Records Creation Method** list, select **Transfer from Server**.
7. In the Records Creation area, type the values for the SOA and NS record parameters.
8. Click **Finished**.

Creating a self IP address using the IP address of the legacy DNS server

To avoid a conflict on your network, unplug BIG-IP® GTM™ from the network.

When you want GTM to handle DNS traffic previously handled by a DNS server, create a self IP address on GTM using the IP address of the legacy DNS server.

1. On the Main tab, click **Network** > **Self IPs**.
   The Self IPs screen opens.
2. Click **Create**.
   The New Self IP screen opens.
3. In the **Name** field, type a unique name for the self IP.
4. In the **IP Address** field, type the IP address of the legacy DNS server.
   The system accepts IPv4 and IPv6 addresses.
5. In the **Netmask** field, type the network mask for the specified IP address.
6. Click **Finished**.
   The screen refreshes, and displays the new self IP address.

Designating GTM as the primary server for the zone

Ensure that you have created a self IP address on BIG-IP® GTM™ using the IP address of the legacy DNS server.

Add this self IP address to the GTM server object, and then modify the DNS server based on your network configuration.

1. On the Main tab, click **DNS** > **GSLB** > **Servers**.
   The Server List screen opens.
2. Click the name of the GTM system that you want to modify.
   The server settings and values display.
3. In the Address List area, add the new self IP address.
4. Click **Update**.
5. Do one of the following based on your network configuration:
   - Modify the IP address of the legacy DNS server so that it becomes a secondary DNS server to BIG-IP GTM. Ensure that the IP address of the DNS server does not conflict with the self IP address that you added to the BIG-IP GTM server object.

     Note: *If you are using BIND servers, and you are unfamiliar with how to change a DNS server from a primary to a secondary, refer to the fifth edition of DNS and BIND, available from O'Reilly Media.*
   - Remove the legacy DNS server from your network.

BIG-IP GTM is now the primary authoritative name server for the zone. The servers for the zone do not need to be updated, because the IP address of the legacy DNS server was assigned to BIG-IP GTM.

Creating listeners to alert GTM to DNS traffic destined for the system

To alert the BIG-IP® GTM™ system to DNS queries (previously handled by the DNS server), create four listeners: two that use the UDP protocol (one each for an IPv4 address and IPv6 address), and two that use the TCP protocol (one each for an IPv4 address and IPv6 address).

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

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 previously used by the legacy DNS server.
5. From the **VLAN Traffic** list, select **All VLANs**.
6. In the Service area, from the **Protocol** list, select **UDP**.
7. 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 a wide IP

Ensure that at least one load balancing pool exists in the configuration before you start creating a wide IP.

Create a wide IP to map a FQDN to one or more pools of virtual servers that host the content of the domain.

1. On the Main tab, click **DNS** > **GSLB** > **Wide IPs**.
   The Wide IP List screen opens.
2. Click **Create**.
   The New Wide IP screen opens.
3. In the **Name** field, type a name for the wide IP.

   Tip: *You can use two different wildcard characters in the wide IP name: asterisk (*) to represent several characters and question mark (?) to represent a single character. This reduces the number of aliases you have to add to the configuration.*

4. From the **Pool** list, select the pools that this wide IP uses for load balancing.
   The system evaluates the pools based on the wide IP load balancing method configured.
   a) From the **Pool** list, select a pool.
      A pool can belong to more than one wide IP.
   b) Click **Add**.
5. Click **Finished**.

Implementation result

BIG-IP® GTM™ replaces the legacy DNS server as the primary authoritative name server for the zone. BIG-IP GTM handles all incoming DNS traffic, whether destined for a wide IP or handled by the BIND instance on the system.

Chapter 7

Placing BIG-IP GTM in Front of a DNS Server

- *Overview: Configuring GTM to screen traffic to an existing DNS server*
- *Task summary*
- *Implementation result*

Overview: Configuring GTM to screen traffic to an existing DNS server

You can use BIG-IP® Global Traffic Manager™ (GTM™) as a traffic screener in front of an existing DNS server. With this setup, all DNS traffic flows through BIG-IP GTM. Listeners that you configure on BIG-IP GTM verify incoming DNS queries. If the query is for a wide IP, BIG-IP GTM resolves the request. If the query is for a destination that does not match a wide IP or for an IP address that is not configured on BIG-IP GTM, the system forwards the query to the specified DNS server for resolution. When forwarding a query, BIG-IP GTM transforms the source address to a self IP address on BIG-IP GTM.

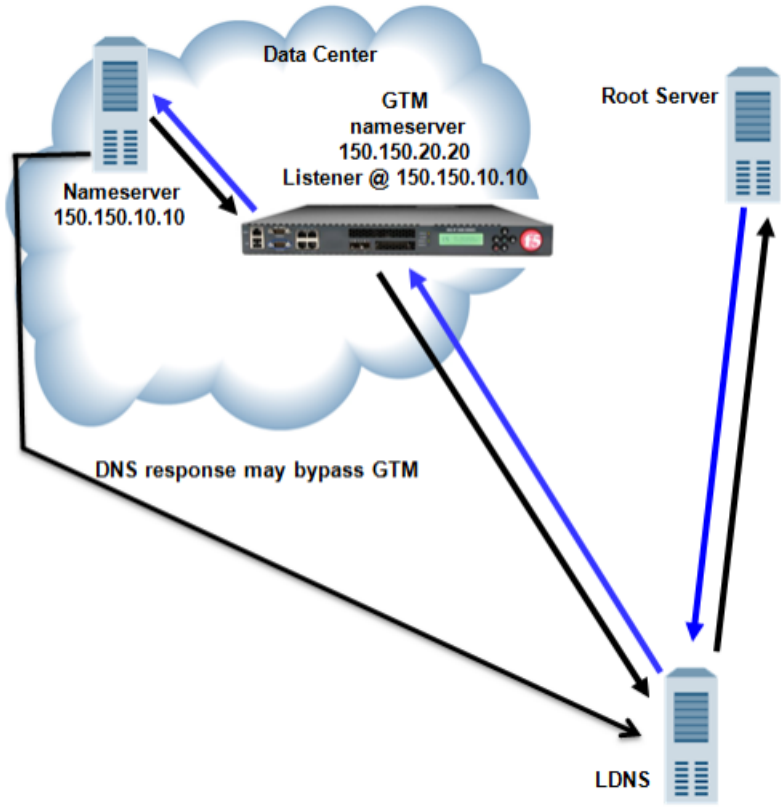

Figure 5: Traffic flow when BIG-IP GTM screens traffic to a DNS server

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 query is sent to the IP address of the listener, BIG-IP GTM™ either handles the request locally or forwards the request to the appropriate resource.

About wildcard listeners

A *wildcard listener* is a special listener that is assigned an IP address of `0.0.0.0` and the DNS query port (port 53). When you want BIG-IP® GTM™ to respond to DNS queries coming into your network, regardless of the destination IP address of the given request, you use a wildcard listener.

Task summary

Perform these tasks to send traffic through BIG-IP® GTM™.

Placing BIG-IP GTM on your network to forward traffic
Creating listeners to forward traffic to a DNS server
Creating a wide IP

Placing BIG-IP GTM on your network to forward traffic

Determine to which DNS server you want BIG-IP® GTM™ to forward traffic.

Place GTM on your network between LDNS servers and clients making DNS name resolution requests.

1. Physically connect GTM to your Internet connection.
2. Connect the LDNS to an Ethernet port on GTM (optional).
3. Connect the LDNS to a switch.

Creating listeners to forward traffic to a DNS server

Determine to which DNS server you want the listeners to forward DNS queries.

Create listeners to alert the BIG-IP system to queries destined for a DNS server. Create four wildcard listeners: two that use the UDP protocol (one each for an IPv4 address and IPv6 address), and two that use the TCP protocol (one each for an IPv4 address and IPv6 address).

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

---

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 DNS queries.

   The destination is the IP address of a DNS server to which you want the listeners to route DNS queries.

   Important: *The destination must not match a self IP address on GTM.*

   ---

5. From the **VLAN Traffic** list, select **All VLANs**.
6. In the Service area, from the **Protocol** list, select **UDP**.
7. 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 a wide IP

Ensure that at least one load balancing pool exists in the configuration before you start creating a wide IP.

Create a wide IP to map a FQDN to one or more pools of virtual servers that host the content of the domain.

1. On the Main tab, click **DNS** > **GSLB** > **Wide IPs**.
   The Wide IP List screen opens.
2. Click **Create**.
   The New Wide IP screen opens.
3. In the **Name** field, type a name for the wide IP.

   Tip: *You can use two different wildcard characters in the wide IP name: asterisk (*) to represent several characters and question mark (?) to represent a single character. This reduces the number of aliases you have to add to the configuration.*

4. From the **Pool** list, select the pools that this wide IP uses for load balancing.
   The system evaluates the pools based on the wide IP load balancing method configured.
   a) From the **Pool** list, select a pool.
      A pool can belong to more than one wide IP.
   b) Click **Add**.
5. Click **Finished**.

Implementation result

You now have an implementation in which BIG-IP®GTM™ receives all DNS queries. If the query is for a wide IP, BIG-IP GTM load balances the request to the appropriate resource. If the query is for an IP address of a DNS server, BIG-IP GTM either routes or forwards the query to the DNS server for resolution.

Chapter 8

Placing BIG-IP GTM in front of a Pool of DNS Servers

- *Overview: Screening and forwarding non-wide IP traffic to a pool of DNS servers*
- *Task summary*
- *Implementation result*

Overview: Screening and forwarding non-wide IP traffic to a pool of DNS servers

BIG-IP® Global Traffic Manager™ (GTM™) can function as a traffic screener in front of a pool of DNS servers. In this situation, BIG-IP GTM checks incoming DNS queries and if the query is for a wide IP, resolves the query. Otherwise, BIG-IP GTM forwards the DNS query to one of the servers in a pool of DNS servers, and that server handles the query.

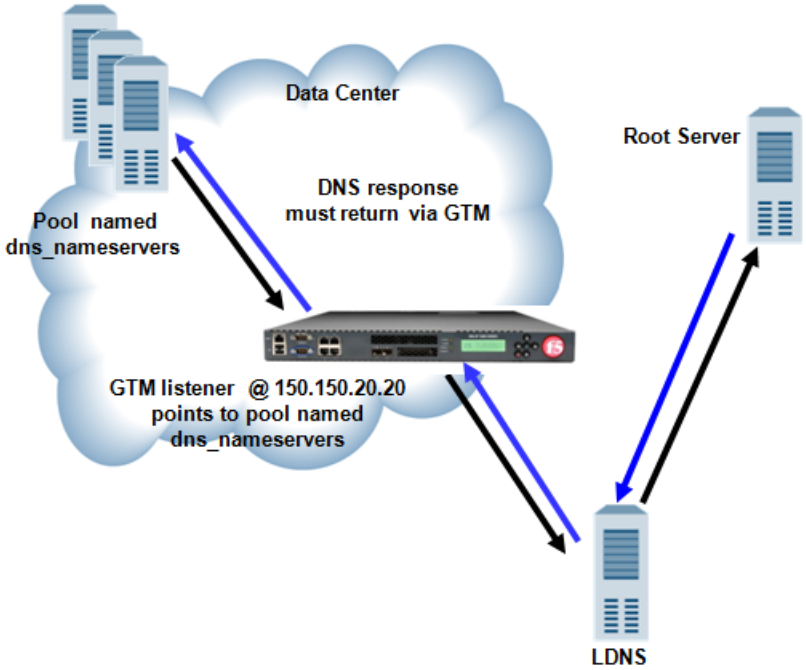

Figure 6: Traffic flow when BIG-IP GTM screens traffic to a pool of DNS servers

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 query is sent to the IP address of the listener, BIG-IP GTM™ either handles the request locally or forwards the request to the appropriate resource.

Task summary

Perform these tasks to screen non-wide IP traffic and forward the traffic to a pool of DNS servers.

Creating a pool of local DNS servers

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

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 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.

Implementation result

You now have an implementation in which BIG-IP® GTM™ receives DNS queries, handles wide IP requests, and forwards all other DNS queries to members of the pool of DNS servers.

Chapter 9

Configuring GTM to Determine PGW Health and Availability

- *Overview: Configuring GTM to determine packet gateway health and availability*

Overview: Configuring GTM to determine packet gateway health and availability

Service providers can configure the BIG-IP® GTM™ system to increase the availability of their customer services on the System Architecture Evolution (SAE) network. One way is to configure a GTP monitor for the health and availability of a packet gateway (PGW). The GTP monitor issues an echo request to a list of PGW systems. If a PGW fails to respond to the GTP echo request, it is marked as down, and removed from the list of available PGW systems that are returned to an MME in a DNS response. GTM can also be configured to load balance DNS queries for the access point name (APN) across the PGW systems that are active and available.

Note: *GTM handles only A and AAAA records for global server load balancing (GSLB).*

This illustration presents a simplified depiction of how the process works on the SAE network.

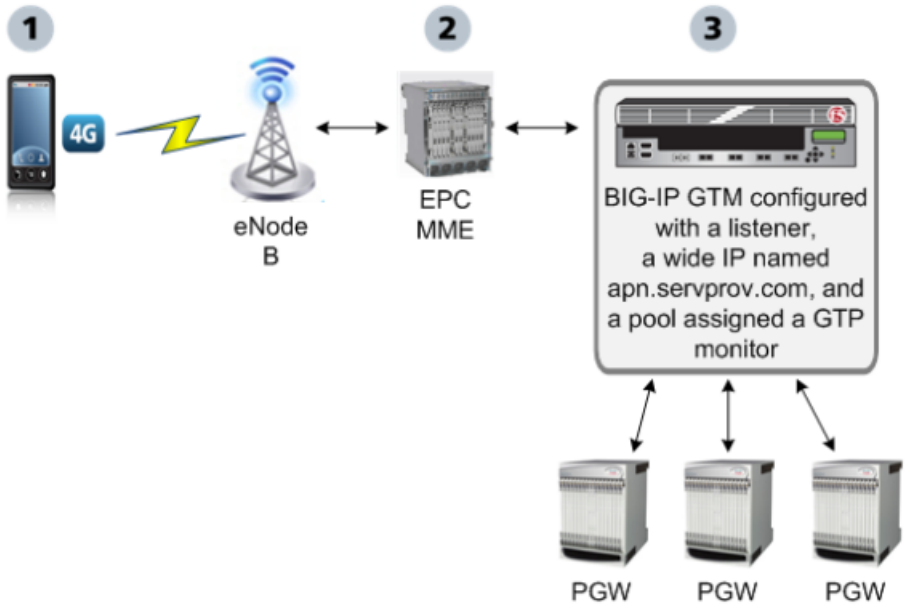

Figure 7: GTM monitoring packet gateways

1. A smartphone that is preprogrammed with an APN, for example, `apn.servprov.com`, initiates a data connection.
2. The EPC MME performs a DNS lookup on `apn.servprov.com` in order to select a packet gateway.
3. GTM handles the DNS request and returns only IP addresses for PGW systems that are active and available.

Task summary

Configure GTM using these tasks to determine PGW system health and availability, and to load balance DNS queries across the active and available PGW systems.

Important: *Before you perform these tasks, ensure that the BIG-IP system is in the PGW trust list.*

Defining a data center
Defining BIG-IP GTM systems

Defining packet gateway systems
Creating listeners to identify DNS traffic for an APN
Creating a custom GTP monitor
Creating a pool of packet gateway systems
Configuring a wide IP for load balancing APN lookups

Defining a data center

On BIG-IP®GTM™, create a data center to contain the servers that reside on a subnet of your network.

1. On the Main tab, click **DNS** > **GSLB** > **Data Centers**.
   The Data Center List screen opens.
2. Click **Create**.
   The New Data Center screen opens.
3. In the **Name** field, type a name to identify the data center.

   Important: *The data center name is limited to 63 characters.*

4. In the **Location** field, type the geographic location of the data center.
5. In the **Contact** field, type the name of either the administrator or the department that manages the data center.
6. From the **State** list, select **Enabled**.
7. Click **Finished**.

Now you can create server objects and assign them to this data center.

Repeat these steps to create additional data centers.

Defining BIG-IP GTM systems

Ensure that at least one data center exists in the configuration before you start creating a server.

On BIG-IP® GTM™, create a server object to represent the GTM system itself.

1. On the Main tab, click **DNS** > **GSLB** > **Servers**.
   The Server List screen opens.
2. Click **Create**.
   The New Server screen opens.
3. In the **Name** field, type a name for the server.

   Important: *Server names are limited to 63 characters.*

4. From the **Product** list, select **BIG-IP System (Single)**.
   The server type determines the metrics that the system can collect from the server.
5. In the Address List area, add the IP addresses of the server.
   You can add more than one IP address, depending on how the server interacts with the rest of your network.

   Important: *You must use a self IP address for a BIG-IP system; you cannot use the management IP address.*

6. From the **Data Center** list, select the data center where the server resides.
7. In the Health Monitors area, assign the **bigip** monitor to the server by moving it from the **Available** list to the **Selected** list.
8. From the **Virtual Server Discovery** list, select how you want virtual servers to be added to the system.

Option	Description
Disabled	The system does not use the discovery feature to automatically add virtual servers. This is the default value. Use this option for a standalone GTM system or for a GTM/LTM® combo system when you plan to manually add virtual servers to the system, or if your network uses multiple route domains.
Enabled	The system uses the discovery feature to automatically add virtual servers. Use this option for a GTM/LTM combo system when you want the GTM system to discover LTM virtual servers.
Enabled (No Delete)	The system uses the discovery feature to automatically add virtual servers and does not delete any virtual servers that already exist. Use this option for a GTM/LTM combo system when you want the GTM system to discover LTM virtual servers.

9. In the Virtual Server List area, if you selected **Disabled** from the **Virtual Server Discovery** list, specify the virtual servers that are resources on this server.
   a) In the **Name** field, type the name of the virtual server.
   b) In the **Address** field, type the IP address of the virtual server.
   c) From the **Service Port** list, select the port the server uses.
   d) Click **Add**.
10. From the **Link Discovery** list, select how you want links to be added to the system.

Option	Description
Disabled	The system does not use the discovery feature to automatically add links. This is the default value. Use this option for a standalone GTM system or for a GTM/LTM combo system when you plan to manually add links to the system.
Enabled	The system uses the discovery feature to automatically add links. Use this option for a GTM/LTM combo system when you want BIG-IP GTM to discover links.
Enabled (No Delete)	The system uses the discovery feature to automatically add links and does not delete any links that already exist. Use this option for a GTM/LTM combo system when you want GTM to discover links.

11. Click **Create**.
    The Server List screen opens displaying the new server in the list.

Defining packet gateway systems

Before you create servers to represent the packet gateway (PGW) systems, ensure there is an existing server in the BIG-IP® GTM™ system that you are configuring.

Define the PGW systems to which BIG-IP GTM load balances access point name (APN) traffic.

1. On the Main tab, click **DNS** > **GSLB** > **Servers**.
   The Server List screen opens.
2. Click **Create**.

The New Server screen opens.

3. In the **Name** field, type a name for the server.

   Important: *Server names are limited to 63 characters.*

4. From the **Product** list, select **Generic Host**.
   The server type determines the metrics that the system can collect from the server.
5. In the Address List area, add the IP addresses of the PGW system.
   a) Type an external (public) IP address in the **Address** field, and then click **Add**.
   b) If you use NAT, type an internal (private) IP address in the **Translation** field, and then click **Add**.

   You can add more than one IP address, depending on how the PGW system interacts with the rest of your network.
6. From the **Data Center** list, select the data center where the server resides.
7. In the Health Monitors area, you can assign the GTP monitor to the server by moving it from the **Available** list to the **Selected** list; however, best practice is to assign the **GTP** monitor to the pool of PGW systems.

   Tip: *The GTP monitor simply checks that the PGW system responds to a GTP echo request.*

8. In the Virtual Server List area, if you selected **Disabled** from the **Virtual Server Discovery** list, create a virtual server to represent (in a pool) the PGW system.
   a) In the **Name** field, type a name for the virtual server.
   b) In the **Address** field, type the IP address of the host server.
   c) In the **Service Port** field, type `2152` (F5 Networks recommends using this GTP-user plane tunneling data port); however, the BIG-IP system also supports the use of `2123` (GTP-control plane port).
   d) Click **Add**.
9. Click **Create**.
   The Server List screen opens displaying the new server in the list.

Define the other PGW systems on your network.

Creating listeners to identify DNS traffic for an APN

Ensure that a self IP address exists on BIG-IP® GTM™ that you can use as the **Destination** of the listener.

Create listeners to identify DNS traffic for a specific access point name (APN). The best practice is to create two listeners: one that handles UDP traffic and one that handles TCP traffic.

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 access point name (APN) traffic.

   Note: *F5 Networks recommends that you assign a unique IP address, not a self IP address.*

5. In the Service area, from the **Protocol** list, select **UDP**.

6. Click **Finished**.

Create another listener with the same IP address, but select **TCP** from the **Protocol** list.

Creating a custom GTP monitor

Ensure that you know the version of the GTP protocol that your network uses.

Create a custom GTP monitor to detect the presence and health of a packet gateway (PGW) system. The GTP monitor issues a GTP echo request, and if the PGW system fails to respond, it is automatically marked as down and removed from the available list of PGW systems that the BIG-IP® system returns to an MME.

1. On the Main tab, click **DNS** > **GSLB** > **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 **GTP**.
5. From the **Import Settings** list, select an existing monitor.
   The new monitor inherits initial configuration values from the existing monitor.
6. Type a number in the **Interval** field that indicates, in seconds, how frequently the system issues the monitor check. The default is `30` seconds.
   The frequency of a monitor check must be greater than the value of the global-level **Heartbeat Interval** setting. Otherwise, the monitor can acquire out-of-date data.
7. Type a number in the **Timeout** field that indicates, in seconds, how much time the target has to respond to the monitor check. The default is `120` seconds.
   If the target responds within the allotted time period, it is considered up. If the target does not respond within the time period, it is considered down.
8. Type a number in the **Probe Interval** field that indicates the number of seconds between the probes sent by the system. The default is `1` second.
9. Type a number in the **Probe Timeout** field that indicates the number of seconds after which the system times out the probe request to the system. The default is `5` seconds.
10. Type a number in the **Probe Attempts** field that indicates the number of probes the system sends before marking the resource down. The default is `3` attempts.
11. Type a number in the **Protocol Version** field that indicates the version of the GTP protocol the system uses. The default is `1`.
12. For the **Ignore Down Response** setting, do one of the following:
    - Accept the **No** default option.
    - Select the **Yes** option to specify that the monitor accepts more than one probe attempt per interval.
13. Click **Finished**.

Now you can associate the new custom monitor with the pool that contains the GTP resources.

Tip: *Associate the monitor only with the pool. If you associate the monitor with both the pool and a server, you might encounter inaccurate health check failures.*

Creating a pool of packet gateway systems

Before you can create a pool of packet gateway (PGW) systems, you need to:

- Create servers to represent the PGW systems, and manually add at least one virtual server to each server.
- Create a GTP monitor.

When you create a pool of one or more PGW systems it is the best practice to apply the GTP monitor and the round robin load-balancing method to the pool; however, the BIG-IP® system supports the use of any static load balancing method in this implementation.

1. On the Main tab, click **DNS** > **GSLB** > **Pools**.
   The Pools list screen opens.
2. Click **Create**.
3. In the **Name** field, type a name for the pool.
   Names must begin with a letter, and can contain only letters, numbers, and the underscore (_) character.

   Important: *The pool name is limited to 63 characters.*

4. For the **Health Monitors** setting, in the **Available** list, select **gtp**, and click **<<** to move the monitor to the **Active** list.
5. In the Load Balancing Method area, from the **Preferred** list, select **Round Robin**.

   Tip: *When deploying this implementation in a lab environment, to determine whether the BIG-IP system returns the DNS response that you expect, try selecting the* ***Global Availability*** *method and disabling the first pool member in the list.*

6. In the Load Balancing Method area, from the **Alternate**, and **Fallback** lists, select a static load balancing method, based on your network environment. Ensure that you select a load balancing method that does not take current server performance or connection load into account.
7. For the Member List setting, add virtual servers as members of this load balancing pool.
   The system evaluates the virtual servers (pool members) in the order in which they are listed. A virtual server can belong to more than one pool.
   a) Select a virtual server from the **Virtual Server** list.
   b) Click **Add**.
8. Click **Finished**.

Configuring a wide IP for load balancing APN lookups

Before you configure a wide IP for an access point name (APN), ensure that a pool of packet gateway (PGW) systems is available to associate with the wide IP that you are configuring for APN load balancing.

Configure a wide IP to represent the APN for which BIG-IP® GTM™ load balances DNS lookups across the PGW systems on your network.

1. On the Main tab, click **DNS** > **GSLB** > **Wide IPs**.
   The Wide IP List screen opens.
2. Click **Create**.
   The New Wide IP screen opens.
3. In the **Name** field, type the APN, for example `apn.servprov.com`.

4. From the **Load Balancing Method** list, select **Round Robin**.
5. From the **Pool** list, select the pool of PGW systems, and then click **Add**.
6. Click **Finished**.

Chapter 10

Configuring GTM on a Network with One Route Domain

- *Overview: How do I deploy BIG-IP GTM on a network with one route domain?*
- *Implementation result*

Overview: How do I deploy BIG-IP GTM on a network with one route domain?

You can deploy BIG-IP® Global Traffic Manager™ (GTM™) on a network where BIG-IP Local Traffic Manager™ (LTM®) is configured with one route domain and no overlapping IP addresses.

Caution: *For BIG-IP systems that include both LTM and GTM, you can configure route domains on internal interfaces only. F5 Networks does not support the configuration of route domains on a standalone BIG-IP GTM.*

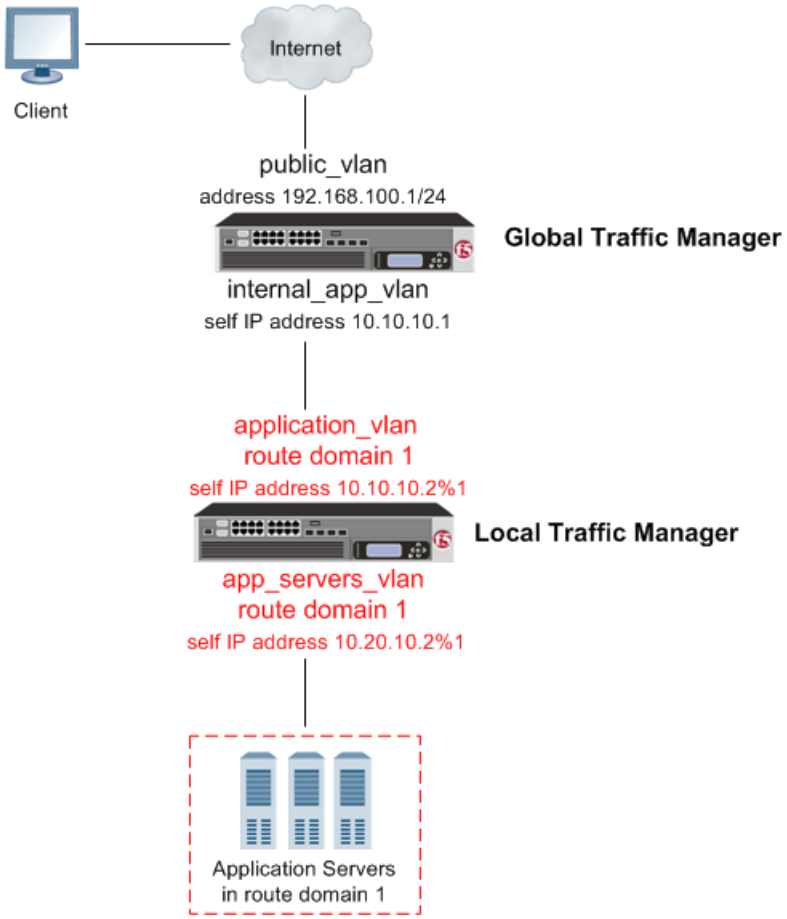

Figure 8: BIG-IP GTM deployed on a network in front of a BIG-IP LTM configured with a route domain

Task summary

Perform these tasks to configure a route domain, and then to configure GTM to be able to monitor the LTM systems.

Creating VLANs for a route domain on BIG-IP LTM
Creating a route domain on the BIG-IP system
Creating a self IP address for a route domain on BIG-IP LTM
Defining a server for a route domain on BIG-IP GTM

Creating VLANs for a route domain on BIG-IP LTM

You need to create two VLANs on BIG-IP® LTM® through which traffic can pass to a route domain.

1. On the Main tab, click **Network** > **VLANs**.
   The VLAN List screen opens.
2. Click **Create**.
   The New VLAN screen opens.
3. In the **Name** field, type `external`.
4. In the **Tag** field, type a numeric tag, from 1-4094, for the VLAN, or leave the field blank if you want the BIG-IP system to automatically assign a VLAN tag.

   The VLAN tag identifies the traffic from hosts in the associated VLAN.
5. For the **Interfaces** setting, from the **Available** list, click an interface number or trunk name and add the selected interface or trunk to the **Untagged** list. Repeat this step as necessary.
6. If you want the system to verify that the return route to an initial packet is the same VLAN from which the packet originated, select the **Source Check** check box.
7. Click **Finished**.
   The screen refreshes, and displays the new VLAN from the list.

Repeat this procedure, but in Step 3, name the VLAN `internal`.

Creating a route domain on the BIG-IP system

Before you create a route domain:

- Ensure that an external and an internal VLAN exist on the BIG-IP® system.
- If you intend to assign a static bandwidth controller policy to the route domain, you must first create the policy. You can do this using the BIG-IP Configuration utility.
- Verify that you have set the current partition on the system to the partition in which you want the route domain to reside.

You can create a route domain on BIG-IP system to segment (isolate) traffic on your network. Route domains are useful for multi-tenant configurations.

1. On the Main tab, click **Network** > **Route Domains**.
   The Route Domain List screen opens.
2. Click **Create**.
   The New Route Domain screen opens.
3. In the **Name** field, type a name for the route domain.

   This name must be unique within the administrative partition in which the route domain resides.
4. In the **ID** field, type an ID number for the route domain.

   This ID must be unique on the BIG-IP system; that is, no other route domain on the system can have this ID.
5. In the **Description** field, type a description of the route domain.
   For example: `This route domain applies to traffic for application MyApp.`
6. For the **Strict Isolation** setting, select the **Enabled** check box to restrict traffic in this route domain from crossing into another route domain.
7. For the **Parent Name** setting, retain the default value.
8. For the **VLANs** setting, from the **Available** list, select a VLAN name and move it to the **Members** list.

Select the VLAN that processes the application traffic relevant to this route domain.

Configuring this setting ensures that the BIG-IP system immediately associates any self IP addresses pertaining to the selected VLANs with this route domain.

9. For the **Dynamic Routing Protocols** setting, from the **Available** list, select one or more protocol names and move them to the **Enabled** list.

   You can enable any number of listed protocols for this route domain. This setting is optional.

10. From the **Bandwidth Controller** list, select a static bandwidth control policy to enforce a throughput limit on traffic for this route domain.
11. From the **Partition Default Route Domain** list, select either **Another route domain (0) is the Partition Default Route Domain** or **Make this route domain the Partition Default Route Domain**.

    This setting does not appear if the current administrative partition is partition `Common`.

    When you configure this setting, either route domain `0` or this route domain becomes the default route domain for the current administrative partition.
12. Click **Finished**.
    The system displays a list of route domains on the BIG-IP system.

You now have another route domain on the BIG-IP system.

Creating a self IP address for a route domain on BIG-IP LTM

Ensure that external and internal VLANs exist on BIG-IP® LTM®, before you begin creating a self IP address for a route domain.

Create a self IP address on LTM that resides in the address space of the route domain.

1. On the Main tab, click **Network** > **Self IPs**.
   The Self IPs screen opens.
2. Click **Create**.
   The New Self IP screen opens.
3. In the **Name** field, type a unique name for the self IP.
4. In the **IP Address** field, type an IP address.

   This IP address must represent a self IP address in a route domain. Use the format `x.x.x.x%n`, where `n` is the route domain ID, for example, 10.1.1.1%1.

   The system accepts IPv4 and IPv6 addresses.
5. In the **Netmask** field, type the network mask for the specified IP address.
6. From the **VLAN/Tunnel** list, select **external**.
7. From the **Port Lockdown** list, select **Allow Default**.
8. Click **Finished**.
   The screen refreshes, and displays the new self IP address.

Repeat all steps, but in Step 6 (from the **VLAN/Tunnel** list) select VLAN **internal**.

Defining a server for a route domain on BIG-IP GTM

Ensure that at least one data center exists in the configuration.

On a BIG-IP® GTM™ system, define a server that represents the route domain.

1. On the Main tab, click **DNS** > **GSLB** > **Servers**.
   The Server List screen opens.
2. Click **Create**.
   The New Server screen opens.
3. In the **Name** field, type a name for the server.

   Important: *Server names are limited to 63 characters.*

4. From the **Product** list, select either **BIG-IP System (Single)** or **BIG-IP System (Redundant)**.
   The server type determines the metrics that the system can collect from the server.
5. In the Address List area, add the self IP address that you assigned to the VLAN that you assigned to the route domain.

   Important: *Do not include the route domain ID in this IP address. Use the format x.x.x.x, for example, 10.10.10.1.*

6. From the **Data Center** list, select the data center where the server resides.
7. In the Health Monitors area, assign the **bigip** monitor to the server by moving it from the **Available** list to the **Selected** list.
8. From the **Virtual Server Discovery** list, select how you want virtual servers to be added to the system.
   Virtual server discovery is supported when you have only one route domain.

Option	Description
Disabled	Use this option when you plan to manually add virtual servers to the system, or if your network uses multiple route domains. This is the default value.
Enabled	The system automatically adds virtual servers using the discovery feature.
Enabled (No Delete)	The system uses the discovery feature and does not delete any virtual servers that already exist.

9. Click **Create**.
   The Server List screen opens displaying the new server in the list.

Implementation result

You now have an implementation in which BIG-IP® GTM™ can monitor virtual servers on BIG-IP LTM® systems configured with one route domain.

Chapter 11

Configuring GTM on a Network with Multiple Route Domains

- *Overview: How do I deploy BIG-IP GTM on a network with multiple route domains?*
- *Implementation result*

Overview: How do I deploy BIG-IP GTM on a network with multiple route domains?

You can deploy BIG-IP® Global Traffic Manager™ (GTM) on a network where BIG-IP Local Traffic Manager™ (LTM®) systems are configured with multiple route domains and overlapping IP addresses.

Important: *On a network with route domains, you must ensure that virtual server discovery (autoconf) is disabled, because virtual server discovery does not discover translation IP addresses.*

Caution: *For BIG-IP systems that include both LTM and GTM, you can configure route domains on internal interfaces only. F5 Networks does not support the configuration of route domains on a standalone BIG-IP GTM.*

The following figure shows BIG-IP GTM deployed in a network with multiple BIG-IP Local Traffic Manager™ (LTM®) systems configured with the default route domain (zero), and two additional route domains. BIG-IP GTM can monitor the Application1 and Application2 servers that have overlapping IP addresses and reside in different route domains. The firewalls perform the required address translation between the BIG-IP GTM and BIG-IP LTM addresses; you must configure the firewalls to segment traffic and avoid improperly routing packets between route domain 1 and route domain 2.

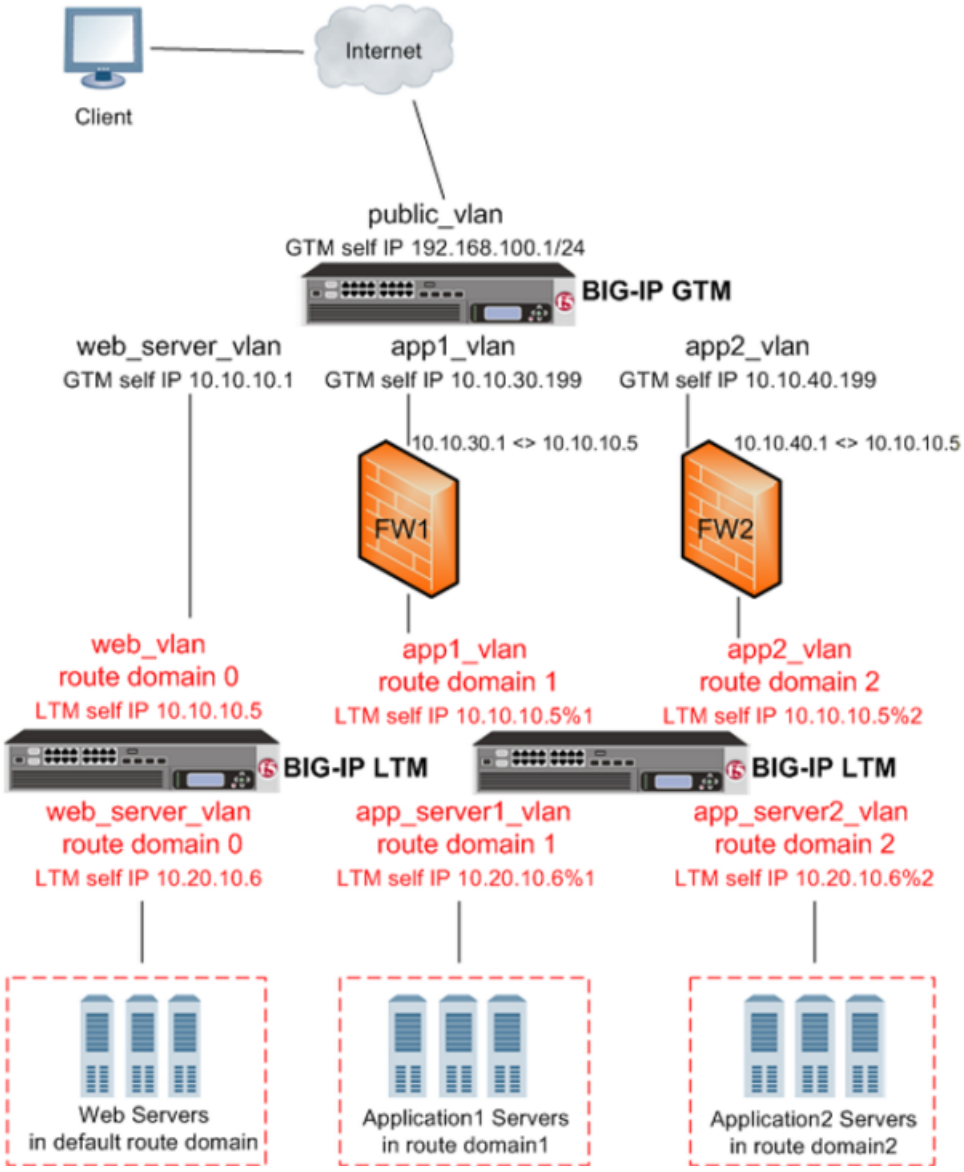

Figure 9: BIG-IP GTM deployed on a network with multiple route domains

Before BIG-IP® GTM™ can gather status and statistics for the virtual servers hosted on BIG-IP LTM® systems on your network that are configured with route domains, you must configure the following on each BIG-IP LTM that handles traffic for route domains:

- VLANs through which traffic for your route domains passes
- Route domains that represent each network segment
- Self IP addresses that represent the address spaces of the route domains

Additionally, on BIG-IP GTM you must:

- Configure, for each route domain, a server object with virtual server discovery disabled
- Disable virtual server discovery globally

Task summary

Perform the following tasks to configure BIG-IP GTM to monitor BIG-IP LTM systems with route domains.

Creating VLANs for a route domain on BIG-IP LTM

Creating a route domain on BIG-IP LTM
Creating a self IP address for a route domain on BIG-IP LTM
Disabling auto-discovery at the global-level on BIG-IP GTM
Defining a server for a route domain on BIG-IP GTM

Creating VLANs for a route domain on BIG-IP LTM

Create two VLANs on BIG-IP® LTM® through which traffic can pass to a route domain.

1. On the Main tab, click **Network** > **VLANs**.
   The VLAN List screen opens.
2. Click **Create**.
   The New VLAN screen opens.
3. In the **Name** field, type `external`.
4. In the **Tag** field, type a numeric tag, from 1-4094, for the VLAN, or leave the field blank if you want the BIG-IP system to automatically assign a VLAN tag.

   The VLAN tag identifies the traffic from hosts in the associated VLAN.
5. For the **Interfaces** setting, from the **Available** list, click an interface number or trunk name and add the selected interface or trunk to the **Untagged** list. Repeat this step as necessary.
6. If you want the system to verify that the return route to an initial packet is the same VLAN from which the packet originated, select the **Source Check** check box.
7. Click **Finished**.
   The screen refreshes, and displays the new VLAN from the list.

Repeat this procedure, but in Step 3, name the second VLAN `internal`.

Creating a route domain on BIG-IP LTM

Ensure that VLANs exist on BIG-IP® LTM®, before you create a route domain.

You can create a route domain on a BIG-IP system to segment (isolate) network traffic on your network.

1. On the Main tab, click **Network** > **Route Domains**.
   The Route Domain List screen opens.
2. Click **Create**.
   The New Route Domain screen opens.
3. In the **ID** field, type an ID number for the route domain.

   This ID must be unique on the BIG-IP system; that is, no other route domain on the system can have this ID.
4. In the **Description** field, type a description of the route domain.
   For example: `This route domain applies to traffic for application MyApp.`
5. For the **Strict Isolation** setting, select the **Enabled** check box to restrict traffic in this route domain from crossing into another route domain.
6. For the **Parent Name** setting, retain the default value.
7. For the **VLANs** setting, move the **external** and **internal** VLANs from the **Available** list, to the **Members** list.

   Configuring this setting ensures that the BIG-IP system immediately associates any self IP addresses pertaining to the selected VLANs with this route domain.

8. Click **Finished**.
   The system displays a list of route domains on the BIG-IP system.

Create additional route domains based on your network configuration.

Creating a self IP address for a route domain on BIG-IP LTM

Ensure that VLANs exist on BIG-IP®LTM®, before you begin creating a self IP address for a route domain.

Create a self IP address on the BIG-IP system that resides in the address space of the route domain.

1. On the Main tab, click **Network** > **Self IPs**.
   The Self IPs screen opens.
2. Click **Create**.
   The New Self IP screen opens.
3. In the **Name** field, type a unique name for the self IP.
4. In the **IP Address** field, type an IP address.

   This IP address must represent a self IP address in a route domain. Use the format `x.x.x.x%n`, where `n` is the route domain ID, for example, 10.1.1.1%1.

   The system accepts IPv4 and IPv6 addresses.
5. In the **Netmask** field, type the network mask for the specified IP address.
6. From the **VLAN/Tunnel** list, select the VLAN that you assigned to the route domain that contains this self IP address.
7. From the **Port Lockdown** list, select **Allow Default**.
8. Click **Finished**.
   The screen refreshes, and displays the new self IP address.

Create additional self IP addresses based on your network configuration.

Disabling auto-discovery at the global-level on BIG-IP GTM

On BIG-IP® GTM™, disable auto-discovery at the global-level.

1. On the Main tab, click **DNS** > **Settings** > **GSLB** > **General**.
   The general Configuration screen opens.
2. Clear the **Auto-Discover** check box.
3. Click **Update**.

Defining a server for a route domain on BIG-IP GTM

Ensure that at least one data center exists in the configuration.

On BIG-IP® GTM™, define a server that represents the route domain.

1. On the Main tab, click **DNS** > **GSLB** > **Servers**.
   The Server List screen opens.
2. Click **Create**.
   The New Server screen opens.

3. In the **Name** field, type a name for the server.

   Important: *Server names are limited to 63 characters.*

4. From the **Product** list, select either **BIG-IP System (Single)** or **BIG-IP System (Redundant)**.
   The server type determines the metrics that the system can collect from the server.
5. In the Address List area, add the self IP address that you assigned to the VLAN that you assigned to the route domain.

   Important: *Do not include the route domain ID in this IP address. Use the format x.x.x.x, for example, 10.10.10.1.*

6. From the **Data Center** list, select the data center where the server resides.
7. From the **Prober Pool** list, select one of the following.

Option	Description
Inherit from Data Center	By default, a server inherits the Prober pool assigned to the data center in which the server resides.
Prober pool name	Select the Prober pool that contains the BIG-IP systems that you want to perform monitor probes of this server.

   Note: *The selected Prober pool must reside in the same route domain as the servers you want the pool members to probe.*

8. In the Health Monitors area, assign the **bigip** monitor to the server by moving it from the **Available** list to the **Selected** list.
9. From the **Virtual Server Discovery** list, select **Disabled**.
10. Click **Create**.
    The New Server screen opens.

Implementation result

You now have an implementation in which BIG-IP GTM monitors BIG-IP LTM virtual servers on the various route domains in your network.

Chapter 12

Setting Up a BIG-IP GTM Redundant System Configuration

- *Overview: Configuring a BIG-IP GTM redundant system*

Overview: Configuring a BIG-IP GTM redundant system

You can configure BIG-IP® Global Traffic Manager™ (GTM™) in a redundant system configuration, which is a set of two BIG-IP GTM systems: one operating as the active unit, the other operating as the standby unit. If the active unit goes offline, the standby unit immediately assumes responsibility for managing DNS traffic. The new active unit remains active until another event occurs that would cause the unit to go offline, or you manually reset the status of each unit.

Task Summary

Perform the following tasks to configure a BIG-IP GTM redundant system configuration.

Before you begin, ensure that the Setup utility was run on both devices. During the Setup process, you create VLANs internal and external and the associated floating and non-floating IP addresses, and VLAN HA and the associated non-floating self IP address. You also configure the devices to be in an active-standby redundant system configuration.

Defining an NTP server
Creating listeners to identify DNS traffic
Defining a data center
Defining a server to represent each BIG-IP system
Enabling global traffic configuration synchronization
Running the gtm_add script

Defining an NTP server

Define a Network Time Protocol (NTP) server that both BIG-IP® GTM™ systems use during configuration synchronization.

Important: *Perform these steps on both the active and standby systems.*

1. On the Main tab, click **System** > **Configuration** > **Device** > **NTP**.
   The NTP Device configuration screen opens.
2. In the Time Server Lookup List area, in the **Address** field, type the IP address of the NTP that you want to add. Then, click **Add**.

   Note: *If you did not disable DHCP before the first boot of the BIG-IP system, and if the DHCP server provides the information about your NTP server, then this field is automatically populated.*
3. Click **Update**.

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.

Defining a data center

On BIG-IP®GTM™, create a data center to contain the servers that reside on a subnet of your network.

1. On the Main tab, click **DNS** > **GSLB** > **Data Centers**.
   The Data Center List screen opens.
2. Click **Create**.
   The New Data Center screen opens.
3. In the **Name** field, type a name to identify the data center.

   Important: *The data center name is limited to 63 characters.*

4. In the **Location** field, type the geographic location of the data center.
5. In the **Contact** field, type the name of either the administrator or the department that manages the data center.
6. From the **State** list, select **Enabled**.
7. Click **Finished**.

Now you can create server objects and assign them to this data center.

Repeat these steps to create additional data centers.

Defining a server to represent each BIG-IP system

Ensure that the data centers where the BIG-IP® GTM™ systems reside exist in the configuration.

Using this procedure, create two servers on the active BIG-IP system, one that represents the active system and one that represents the standby system.

Important: *Perform this procedure on only the active system.*

1. On the Main tab, click **DNS** > **GSLB** > **Servers**.
   The Server List screen opens.
2. Click **Create**.
   The New Server screen opens.
3. In the **Name** field, type a name for the server.

   Important: *Server names are limited to 63 characters.*

4. From the **Product** list, select **BIG-IP System (Redundant)**.
   The server type determines the metrics that the system can collect from the server.
5. In the Address List area, add the IP address of the server.

   Important: *You must use a self IP address for a BIG-IP® system; you cannot use the management IP address.*

6. In the Address List area, add the IP addresses of the back up system using the **Peer Address List** setting.
   a) Type an external (public) IP address in the **Address** field, and then click **Add**.
   b) Type an internal (private) IP address in the **Translation** field, and then click **Add**.

   You can add more than one IP address, depending on how the server interacts with the rest of your network.
7. From the **Data Center** list, select the data center where the server resides.
8. From the **Virtual Server Discovery** list, select **Disabled**.
9. Click **Create**.
   The Server List screen opens displaying the new server in the list.

Enabling global traffic configuration synchronization

Enable global traffic configuration synchronization options and assign a name to the GTM synchronization group.

1. On the Main tab, click **DNS** > **Settings** > **GSLB** > **General**.
   The General configuration screen opens.
2. Select the **Synchronize** check box.
3. In the **Group Name** field, type the name of the synchronization group.
4. In the **Time Tolerance** field, type the maximum number of seconds allowed between the time settings on this system and the other systems in the synchronization group.
   The lower the value, the more often this system makes a log entry indicating that there is a difference.

   Tip: *If you are using NTP, leave this setting at the default value of* `10`*. In the event that NTP fails, the system uses the time_tolerance variable to maintain synchronization.*

5. Select the **Synchronize DNS Zone Files** check box.
6. Click **Update**.

Running the gtm_add script

You must run the `gtm_add` script from the standby system.

Note: *You must perform this task from the command-line interface.*

---

1. On the new BIG-IP® GTM™ system, log in to the command-line interface.
2. Type `gtm_add`, and press Enter.
3. Press the y key to start the `gtm_add` script.
4. Type the IP address of the existing GTM system, and press Enter.

The `gtm_add` script acquires configuration data from the active system; once this process completes, you have successfully created a redundant system consisting of two GTM systems.

Chapter
13

Authenticating with SSL Certificates Signed by a Third Party

- *Overview: Authenticating with SSL certificates signed by a third party*
- *Configuring Level 1 SSL authentication*
- *Implementation Results*
- *Configuring certificate chain SSL authentication*
- *Implementation result*

Overview: Authenticating with SSL certificates signed by a third party

BIG-IP® systems use Secure Sockets Layer (SSL) authentication to verify the authenticity of the credentials of systems with which data exchange is necessary.

BIG-IP software includes a self-signed SSL certificate. If your network includes one or more certificate authority (CA) servers, you can also install SSL certificates that are signed by a third party. The BIG-IP systems exchange SSL certificates, and use a CA server to verify the authenticity of the certificates.

The `big3d` agent on all BIG-IP systems and the `gtmd` agent on BIG-IP Global Traffic Manager™ (GTM™) systems use the certificates to authenticate communication between the systems.

About SSL authentication levels

SSL supports ten levels of authentication (also known as certificate depth):

- Level 0 certificates (self-signed certificates) are verified by the system to which they belong.
- Level 1 certificates are authenticated by a CA server that is separate from the system.
- Levels 2 - 9 certificates are authenticated by additional CA servers that verify the authenticity of other servers. These multiple levels of authentication (referred to as *certificate chains*) allow for a tiered verification system that ensures that only authorized communications occur between servers.

Configuring Level 1 SSL authentication

You can configure BIG-IP® systems for Level 1 SSL authentication. Before you begin, ensure that the systems you are configuring include the following:

- A signed certificate/key pair.
- The root certificate from the CA server.

Task Summary

Importing the device certificate
Importing the root certificate for the gtmd agent
Importing the root certificate for the big3d agent
Verifying the certificate exchange

Importing the device certificate

To configure the BIG-IP® system for Level 1 SSL authentication, import the device certificate signed by the CA server.

Note: *Perform this procedure on all BIG-IP® systems that you want to handle Level 1 SSL authentication.*

1. On the Main tab, click **System** > **Device Certificates**.
   The Device Certificate screen opens.
2. Click **Import**.

3. From the **Import Type** list, select **Certificate and Key**.
4. For the **Certificate Source** setting, select **Upload File** and browse to select the certificate signed by the CA server.
5. For the **Key Source** setting, select **Upload File** and browse to select the device key file.
6. Click **Import**.

Importing the root certificate for the gtmd agent

Before you start this procedure, ensure that you have the root certificate from your CA server available.

To set up the system to use a third-party certificate signed by a CA server, replace the existing certificate file for the `gtmd` agent with the root certificate of your CA server.

Note: *Perform this procedure on only one BIG-IP® GTM™ system in the GTM synchronization group. The system automatically synchronizes the setting with the other systems in the group.*

1. On the Main tab, click **DNS** > **GSLB** > **Servers** > **Trusted Server Certificates**.
   The Trusted Server Certificates screen opens.
2. Click **Import**.
3. From the **Import Method** list, select **Replace**.
4. For the **Certificate Source** setting, select **Upload File** and browse to select the root certificate file.
5. Click **Import**.

Importing the root certificate for the big3d agent

Before you start this procedure, ensure that the root certificate from your CA server is available.

Note: *Perform this procedure on all BIG-IP® systems that you want to configure for Level 1 SSL authentication.*

1. On the Main tab, click **System** > **Device Certificates** > **Trusted Device Certificates**.
   The Trusted Device Certificates screen opens.
2. Click **Import**.
3. From the **Import Method** list, select **Replace**.
4. For the **Certificate Source** setting, select **Upload File** and browse to select the certificate signed by the CA server.
5. Click **Import**.

Verifying the certificate exchange

You can verify that you installed the certificate correctly, by running the following commands on all BIG-IP® systems that you configured for Level 1 SSL authentication.

```
iqdump <IP address of BIG-IP you are testing>
iqdump <IP address of BIG-IP peer system, if testing a redundant system
configuration>
```

If the certificate was installed correctly, these commands display a continuous stream of information.

Implementation Results

The BIG-IP® systems are now configured for Level 1 SSL authentication.

Configuring certificate chain SSL authentication

You can configure BIG-IP® systems for certificate chain SSL authentication.

Task Summary

Creating a certificate chain file
Importing the device certificate from the last CA server in the chain
Importing a certificate chain file for the gtmd agent
Importing a certificate chain for the big3d agent
Verifying the certificate chain exchange

Creating a certificate chain file

Before you start this procedure, ensure that you have the certificate files from your CA servers available.

Create a certificate chain file that you can use to replace the existing certificate file.

1. Using a text editor, create an empty file for the certificate chain.
2. Still using a text editor, copy an individual certificate from its own certificate file and paste the certificate into the file you created in step 1.
3. Repeat step 2 for each certificate that you want to include in the certificate chain.

You now have a certificate chain file.

Importing the device certificate from the last CA server in the chain

Import the device certificate signed by the last CA in the certificate chain.

Note: *Perform this procedure on all BIG-IP systems that you want to configure for certificate chain SSL authentication.*

1. On the Main tab, click **System** > **Device Certificates**.
   The Device Certificate screen opens.
2. Click **Import**.
3. From the **Import Type** list, select **Certificate and Key**.
4. For the **Certificate Source** setting, select **Upload File** and browse to select the certificate signed by the CA server.
5. For the **Key Source** setting, select **Upload File** and browse to select the device key file.

6. Click **Import**.

Importing a certificate chain file for the gtmd agent

Before importing a certificate chain file for the gtmd agent, ensure that you have the certificate chain file available.

Replace the existing certificate file on the system with a certificate chain file.

Note: *Perform these steps on only one BIG-IP® GTM™ in a GTM synchronization group. The system automatically synchronizes the setting with the other systems in the group.*

---

1. On the Main tab, click **DNS** > **GSLB** > **Servers** > **Trusted Server Certificates**.
   The Trusted Server Certificates screen opens.
2. Click **Import**.
3. From the **Import Method** list, select **Replace**.
4. For the **Certificate Source** setting, select **Upload File** and browse to select the device certificate for the last CA in the certificate chain.
5. Click **Import**.

Importing a certificate chain for the big3d agent

Before importing a certificate chain for the big3d agent, ensure that the certificate chain file is available.

Note: *Perform these steps on all BIG-IP® systems that you want to configure for certificate chain SSL authentication.*

---

1. On the Main tab, click **System** > **Device Certificates** > **Trusted Device Certificates**.
   The Trusted Device Certificates screen opens.
2. Click **Import**.
3. From the **Import Method** list, select **Replace**.
4. For the **Certificate Source** setting, select **Upload File** and browse to select the certificate chain file.
5. Click **Import**.

Verifying the certificate chain exchange

You can verify that you installed the certificate chain correctly, by running the following commands on all the systems you configure for certificate chain SSL authentication.

```
iqdump <IP address of BIG-IP you are testing>
iqdump <IP address of BIG-IP peer system, if testing a redundant system
configuration>
```

If the certificate chain was installed correctly, these commands display a continuous stream of information.

Implementation result

The BIG-IP® systems are now configured for certificate chain SSL authentication. For information about troubleshooting BIG-IP device certificates, see SOL8187 on AskF5.com (`www.askf5.com`).

Chapter 14

Configuring a TTL in a DNS NoError Response

- *Overview: Configuring a TTL in an IPv6 DNS NoError Response*
- *Task summary*
- *Implementation result*

Overview: Configuring a TTL in an IPv6 DNS NoError Response

You can configure BIG-IP® GTM™ to return IPv6 DNS NoError responses that include a TTL. With this configuration, local DNS servers can cache a negative response. Negative caching reduces both the response time for negative DNS responses and the number of messages that must be sent between resolvers and local DNS servers.

About SOA records and negative caching

A start of authority *SOA* record contains a TTL by which a local DNS server can be configured to cache a DNS NoError response to an IPv6 query.

Task summary

You can configure GTM™ to provide a negative caching TTL for a domain name by performing these specific tasks.

Creating a pool

Creating a wide IP that provides for negative caching

Creating a pool

Ensure that at least one virtual server exists in the configuration before you start to create a load balancing pool.

Create a pool to which the system can load balance global traffic.

1. On the Main tab, click **DNS** > **GSLB** > **Pools**.
   The Pools list screen opens.
2. Click **Create**.
3. In the **Name** field, type a name for the pool.
   Names must begin with a letter, and can contain only letters, numbers, and the underscore (_) character.

   Important: *The pool name is limited to 63 characters.*
4. For the **Health Monitors** setting, in the **Available** list, select a monitor type, and click **<<** to move the monitor to the **Active** list.

   Tip: *Hold the Shift or Ctrl key to select more than one monitor at a time.*
5. For the Member List setting, add virtual servers as members of this load balancing pool.
   The system evaluates the virtual servers (pool members) in the order in which they are listed. A virtual server can belong to more than one pool.
   a) Select a virtual server from the **Virtual Server** list.
   b) Click **Add**.

6. Click **Finished**.

Creating a wide IP that provides for negative caching

Ensure that at least one global load balancing pool exists in the configuration before you create a wide IP.

Create a wide IP configured in a manner where BIG-IP® GTM™ returns an SOA record that contains a TTL with an IPv6 DNS NoError response. With this configuration, the local DNS servers can cache a negative response and thus provide faster responses to DNS queries.

1. On the Main tab, click **DNS** > **GSLB** > **Wide IPs**.
   The Wide IP List screen opens.
2. Click **Create**.
   The New Wide IP screen opens.
3. From the General Properties list, select **Advanced**.
4. In the **Name** field, type a name for the wide IP.

   Tip: *You can use two different wildcard characters in the wide IP name: asterisk (*) to represent several characters and question mark (?) to represent a single character. This reduces the number of aliases you have to add to the configuration.*

5. From the **IPv6 NoError Response** list, select **Enabled**.
   With this option enabled, the system responds faster to IPv6 requests for which it does not have AAAA records configured.
6. In the **IPv6 NoError TTL** field, type the number of seconds that the local DNS servers consider the IPv6 NoError response to be valid. When you set this value, you must enable the **IPv6 NoError Response** setting as well.
7. From the **Pool** list, select the pools that this wide IP uses for load balancing.
   The system evaluates the pools based on the wide IP load balancing method configured.
   a) From the **Pool** list, select a pool.
      A pool can belong to more than one wide IP.
   b) Click **Add**.
8. Click **Finished**.

Implementation result

You now have an implementation in which GTM™ returns a TTL in an IPv6 DNS NoError response for a web site represented by a wide IP in the GTM configuration.

Chapter 15

Configuring Device-Specific Probing and Statistics Collection

- *Overview: Configuring device-specific probing and statistics collection*
- *Task summary*
- *Implementation result*

Overview: Configuring device-specific probing and statistics collection

BIG-IP® Global Traffic Manager™ (GTM™) performs intelligent probing of your network resources to determine whether the resources are up or down. In some circumstances, for example, if your network contains firewalls, you might want to set up device-specific probing to specify which BIG-IP® systems probe specific servers for health and performance data.

About Prober pools

A *Prober pool* is an ordered collection of one or more BIG-IP® systems. BIG-IP Global Traffic Manager™ (GTM™) can be a member of more than one Prober pool, and a Prober pool can be assigned to an individual server or a data center. When you assign a Prober pool to a data center, by default, the servers in that data center inherit that Prober pool.

The members of a Prober pool perform monitor probes of servers to gather data about the health and performance of the resources on the servers. BIG-IP GTM makes load balancing decisions based on the gathered data. If all of the members of a Prober pool are marked down, or if a server has no Prober pool assigned, BIG-IP GTM reverts to a default intelligent probing algorithm to gather data about the resources on the server.

This figure illustrates how Prober pools work. BIG-IP GTM contains two BIG-IP Local Traffic Manager™ (LTM™) systems that are assigned Prober pools and one BIG-IP LTM system that is not assigned a Prober pool:

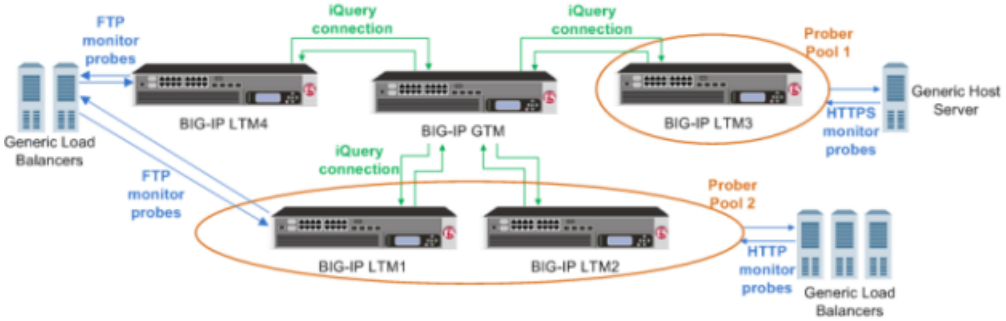

Figure 10: BIG-IP systems with prober pools

Prober Pool 1 is assigned to a generic host server

BIG-IP LTM3 is the only member of Prober Pool 1, and performs all HTTPS monitor probes of the server.

Prober Pool 2 is assigned to generic load balancers

BIG-IP LTM1 and BIG-IP LTM2 are members of Prober Pool 2. These two systems perform HTTP monitor probes of generic load balancers based on the load balancing method assigned to Prober Pool 2.

The generic load balancers on the left side of the graphic are not assigned a Prober pool

BIG-IP GTM can solicit any BIG-IP system to perform FTP monitor probes of these load balancers, including systems that are Prober pool members.

About Prober pool status

The status of a Prober pool also indicates the status of the members of the pool. If at least one member of a Prober pool has green status (Available), the Prober pool has green status.

The status of a Prober pool member indicates whether the BIG-IP GTM™ system, on which you are viewing status, can establish an iQuery connection with the member.

Note: *If a Prober pool member has red status (Offline), no iQuery connection exists between the member and the BIG-IP GTM system on which you are viewing status. Therefore, that BIG-IP GTM system cannot request that member to perform probes, and the Prober pool will not select the member for load balancing.*

About Prober pool statistics

You can view the number of successful and failed probe requests that the BIG-IP® GTM™ system (on which you are viewing statistics) made to the Prober pools. These statistics reflect only the number of Probe requests and their success or failure. These statistics do not reflect the actual probes that the pool members made to servers on your network.

Prober pool statistics are not aggregated among the BIG-IP GTM systems in a synchronization group. The statistics on one BIG-IP GTM include only the requests made from that BIG-IP GTM system.

In this figure, the Prober pool statistics that display on BIG-IP GTM1 are the probe requests made only by that system.

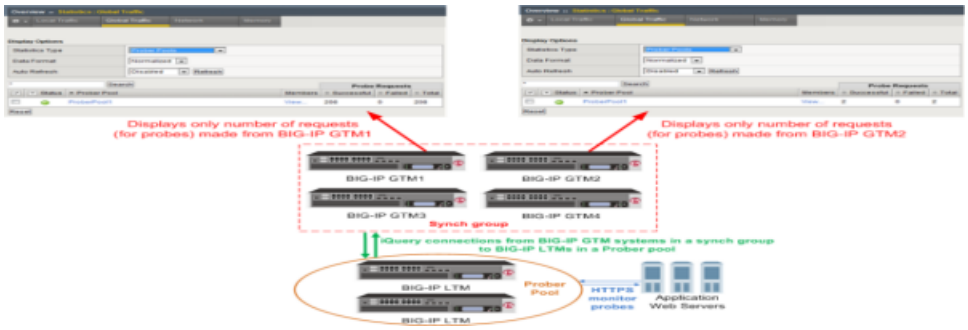

Figure 11: Prober pool statistics displayed per system

Task summary

Perform these tasks to configure device-specific probing and statistics collection.

Defining a data center
Defining a server
Creating a Prober pool
Assigning a Prober pool to a data center
Assigning a Prober pool to a server
Viewing Prober pool statistics and status
Determining which Prober pool member marked a resource down

Defining a data center

On BIG-IP®GTM™, create a data center to contain the servers that reside on a subnet of your network.

1. On the Main tab, click **DNS** > **GSLB** > **Data Centers**.
   The Data Center List screen opens.
2. Click **Create**.
   The New Data Center screen opens.
3. In the **Name** field, type a name to identify the data center.

   Important: *The data center name is limited to 63 characters.*

4. In the **Location** field, type the geographic location of the data center.
5. In the **Contact** field, type the name of either the administrator or the department that manages the data center.
6. From the **State** list, select **Enabled**.
7. Click **Finished**.

Now you can create server objects and assign them to this data center.

Repeat these steps to create additional data centers.

Defining a server

Ensure that at least one data center exists in the configuration.

On BIG-IP® GTM™, define a server that represents a physical server in your network. Repeat these steps for each server in your network, including the GTM itself, other BIG-IP systems, other load balancers, and third-party host servers.

Important: *At a minimum, you must define two servers, one that represents GTM and one that represents another managed server (either a load balancing or host server).*

1. On the Main tab, click **DNS** > **GSLB** > **Servers**.
   The Server List screen opens.
2. Click **Create**.
   The New Server screen opens.
3. In the **Name** field, type a name for the server.

   Important: *Server names are limited to 63 characters.*

4. From the **Product** list, select the server type.

   The server type determines the metrics that the system can collect from the server.

   Note: *If your network uses a server that is not on this list, use the* ***Generic Load Balancer*** *or* ***Generic Host*** *option.*

5. In the Address List area, add the IP addresses of the server.
   a) Type an external (public) IP address in the **Address** field, and then click **Add**.
   b) If you use NAT, type an internal (private) IP address in the **Translation** field, and then click **Add**.

You can add more than one IP address, depending on how the server interacts with the rest of your network.

6. From the **Data Center** list, select the data center where the server resides.
7. In the Health Monitors area, assign health monitors to the server by moving them from the **Available** list to the **Selected** list.

Tip: *If the server is a BIG-IP system, use the* ***bigip*** *monitor. If the server is a generic host, consider using the* ***gateway_icmp*** *monitor, because this monitor simply checks that the server responds to a ping.*

8. From the **Virtual Server Discovery** list, select how you want virtual servers to be added to the system.

Option	Description
Disabled	The system does not use the discovery feature to automatically add virtual servers. This is the default value. Use this option for a standalone GTM system or for a GTM/LTM® combo system when you plan to manually add virtual servers to the system, or if your network uses multiple route domains.
Enabled	The system uses the discovery feature to automatically add virtual servers. Use this option for a GTM/LTM combo system when you want the GTM system to discover LTM virtual servers.
Enabled (No Delete)	The system uses the discovery feature to automatically add virtual servers and does not delete any virtual servers that already exist. Use this option for a GTM/LTM combo system when you want the GTM system to discover LTM virtual servers.

9. Click **Create**.
The Server List screen opens displaying the new server in the list.

Creating a Prober pool

Obtain a list of the BIG-IP® systems in your network and ensure that a server object is configured on the BIG-IP GTM™for each system.

Create a Prober pool that contains the BIG-IP systems that you want to perform monitor probes of a specific server or the servers in a data center.

1. On the Main tab, click **DNS** > **GSLB** > **Prober Pools**.
The Prober Pool List screen opens.
2. Click **Create**.
The New Prober Pool screen opens.
3. In the **Name** field, type a name for the Prober pool.

Important: *Prober pool names are limited to* `63` *characters.*

4. Select a method from the **Load Balancing Method** list.

Option	Description
Round Robin	GTM load balances monitor probes among the members of a Prober pool in a circular and sequential pattern.
Global Availability	GTM selects the first available Prober pool member to perform a monitor probe.

5. Assign members to the pool by moving servers from the **Available** list to the **Selected** list.
6. To reorder the members in the **Selected** list, choose a server and use the **Up** and **Down** buttons to move the server to a different location in the list.

   The order of the servers in the list is important in relation to the load balancing method you selected.
7. Click **Finished**.

Assign the Prober pool to a data center or a server.

Assigning a Prober pool to a data center

Ensure that a Prober pool is available on the system.

To make a specific collection of BIG-IP® systems available to probe the servers in a data center, assign a Prober pool to the data center.

1. On the Main tab, click **DNS** > **GSLB** > **Data Centers**.
   The Data Center List screen opens.
2. Click a data center name.
   The data center settings and values display.
3. From the **Prober Pool** list, select the Prober pool that contains the BIG-IP® systems that you want to perform monitor probes of the servers in this data center.

   By default, all of the servers in the data center inherit this Prober pool.
4. Click **Update**.

Assigning a Prober pool to a server

Ensure that a Prober pool is available on the system.

To specify which BIG-IP® systems perform monitor probes of a server, assign a Prober pool to the server.

1. On the Main tab, click **DNS** > **GSLB** > **Servers**.
   The Server List screen opens.
2. In the Server List, click a server name.
   The server settings and values display.
3. From the **Prober Pool** list, select one of the following.

Option	Description
Inherit from Data Center	By default, a server inherits the Prober pool assigned to the data center in which the server resides.
Prober pool name	Select the Prober pool that contains the BIG-IP systems that you want to perform monitor probes of this server.

4. Click **Update**.

Viewing Prober pool statistics and status

You can view status and statistics for Prober pools and the members of the pools.

1. On the Main tab, click **DNS** > **GSLB** > **Prober Pools**.
   The Prober Pool List screen opens.
2. On the menu bar, click **Statistics**.
   The Global Traffic Statistics screen opens.
3. Click the **Refresh** button.
   The statistics are updated.
4. To view additional information about the status of a Prober pool, place your cursor over the icon in the Status column.
5. To view additional information about the status of a Prober pool member, click **View** in the Members column, and then place your cursor over the icon in the Status column of a specific member.

Determining which Prober pool member marked a resource down

When a resource is marked down, you can open the BIG-IP® GTM™ log to view the SNMP trap and determine which member of a Prober pool marked the resource down.

1. On the Main tab, click **System** > **Logs**.
   The System logs screen opens.
2. On the menu bar, click **Local Traffic**.
   The Local Traffic logs screen opens.
3. You can either scroll through the log or search for a log entry about a specific event.

Implementation result

You now have an implementation in which a specific BIG-IP® system probes the resources on a specific server, or the servers in a specific data center.

Chapter 16

Configuring How and When GTM Saves Configuration Changes

- *Overview: Configuring how and when GTM saves configuration changes*

Overview: Configuring how and when GTM saves configuration changes

By default, BIG-IP® Global Traffic Manager™ (GTM™) automatically saves GTM configuration changes 15 seconds after the change is made in either the Configuration utility or `tmsh`. You can change how long GTM waits before it saves GTM configuration changes. In addition, you can disable automatic saves of GTM configuration changes, but then you must run a command in `tmsh` to save those changes. All changes to the GTM configuration are stored in the `bigip_gtm.conf` file.

Task summary

Perform one of these tasks to configure how and when the BIG-IP system saves GTM configuration changes.

Changing the automatic configuration save timeout
Enabling manual saves of configuration changes
Configuring how and when GTM saves configuration changes using tmsh

Changing the automatic configuration save timeout

Ensure that GTM™ is provisioned on the device.

You can change how long the BIG-IP system waits to save the GTM configuration following a GTM configuration change. For example, if you are making many changes to the GTM configuration at one time, you might want to extend the **Configuration Save Timeout** to allow you to complete more changes before the GTM configuration is saved.

1. On the Main tab, click **DNS** > **Settings** > **GSLB** > **General**.
   The General configuration screen opens.
2. In the Configuration Save area, for the **Automatic** setting, select the **Enabled** check box.
3. In the Configuration Save area, for the **Timeout** field, type the number of seconds that follow a GTM configuration change before the GTM configuration is automatically saved.

   The values shown in the table are worth noting:

Value in seconds	Description
0	GTM immediately saves changes to the configuration.
86400	Maximum number of seconds following a GTM configuration change before the BIG-IP system saves the GTM configuration.
15	Default number of seconds following a GTM configuration change before the BIG-IP system saves the GTM configuration.

Warning: *Setting the value of the* ***Timeout*** *field to less than `10` seconds can impact system performance.*

The BIG-IP system waits the specified number of seconds before saving GTM configuration changes to the stored configuration.

Enabling manual saves of configuration changes

Ensure that GTM™ is provisioned on the device.

You can disable automatic saves of GTM configuration changes when you want to have strict control over when GTM configuration changes are saved to the stored configuration. CPU usage can be affected simply by saving small changes to a large configuration.

1. On the Main tab, click **DNS** > **Settings** > **GSLB** > **General**.
   The General configuration screen opens.
2. In the Configuration Save area, for the Automatic setting, clear the **Enabled** check box to disable automatic saves of GTM configuration changes.

   Important: *If you disable automatic saves of GTM configuration changes, to save those changes you must run this command from the command line:* `tmsh save sys config gtm-only partitions all`
3. Click **Update**.

Configuring how and when GTM saves configuration changes using tmsh

Ensure that GTM™ is provisioned on the device, and that your user role provides access to `tmsh`.

By default, the BIG-IP® system automatically saves GTM configuration changes made in the Configuration utility and `tmsh`. You can change how long the system waits to save GTM configuration changes. You can also configure the system for manual saves that require you to run a `tmsh` command to save GTM configuration changes.

1. Log in to the command-line interface of the BIG-IP system.
2. Run a variation of this command, based on how and when you want the BIG-IP system to save GTM configuration changes:

   ```
   tmsh modify gtm global-settings general automatic-configuration-save-timeout <interval in seconds>
   ```

   Note the value for each save-timeout interval:

Interval in seconds	Value description
0	GTM immediately saves changes to the configuration.
-1	GTM never saves changes to the configuration (manual save required).
86400	Maximum number of seconds following a GTM configuration change before the system saves the change.
15	Default number of seconds following a GTM configuration change before the system saves the change.

   Warning: *Setting* ***automatic-configuration-save-timeout*** *to less than* `10` *seconds can impact system performance.*

GTM waits the number of seconds you specify before saving GTM configuration changes. If you specified `-1`, then you must save the configuration manually using this command: `tmsh save sys config gtm-only partitions all`

Chapter 17

Configuring Logging of Global Server Load Balancing Decisions

- *About logging global server load-balancing decisions*

About logging global server load-balancing decisions

When BIG-IP® GTM™ receives a DNS query for a wide IP, in order to send a response, the system makes a load-balancing decision. The decision is based on the load-balancing method configured on the wide IP, the number of pools associated with the wide IP, and the applicable number of members in each pool.

You can send information about how GTM made the load-balancing decision to the high-speed remote logs; reviewing the logs can help determine how to fine-tune your network.

Configuring logs for global server load-balancing decisions

Ensure that at least one wide IP exists in the BIG-IP® GTM™ configuration, and that high-speed remote logging is configured on the device.

When you want to view the global server load-balancing decisions made by GTM in the high-speed remote logs, configure the verbosity of the information that displays in the logs.

1. On the Main tab, click **DNS** > **GSLB** > **Wide IPs**.
   The Wide IP List screen opens.
2. Click the name of the wide IP you want to modify.
3. From the General Properties list, select **Advanced**.
4. For the **Load-Balancing Decision Log** setting, select the check boxes of the options that you want to include in the high-speed remote logs.

Check-box option	Log information
Pool Selection	The pool selected to answer a DNS request, and why the pool was selected.
Pool Traversal	The pools in the wide IP considered during the load-balancing decision, and why the pool was selected.
Pool Member Selection	The pool member selected to answer a DNS request, and why the member was selected.
Pool Member Traversal	The members of the pool considered during the load-balancing decision, and why the member was selected.

Example log for a wide IP configured for Ratio load balancing when **Load-Balancing Decision Log** is set to only **Pool Selection**: `2013-03-14 15:40:05 bigip1.com to 10.10.10.9#34824: [wip.test.net A] [ratio selected pool (pool_b) with the first highest ratio counter (1)]`

Example log for a wide IP configured for Ratio load balancing when **Load-Balancing Decision Log** is set to both **Pool Selection** and **Pool Traversal**: `2013-03-14 16:18:41 bigip1.com from 10.10.10.9#35902 [wip.test.net A] [ratio selected pool (pool_a) - ratio counter (0) is higher] [ratio skipped pool (pool_b) - ratio counter (0) is not higher] [ratio reset IPv4 ratio counter to original ratios - the best had zero ratio count] [ratio selected pool (pool_a) - ratio counter (1) is not higher] [ratio selected pool (pool_b) - ratio counter (1) is not higher] [ratio selected pool (pool_a) with the first highest ratio counter (1)]`

Chapter 18

Monitoring Third-Party Servers with SNMP

- *Overview: SNMP monitoring of third-party servers*
- *Implementation result*

Overview: SNMP monitoring of third-party servers

You can configure the BIG-IP® Global Traffic Manager™ (GTM™) to acquire information about the health of a third-party server using SNMP. The server must be running an SNMP agent.

Task summary

To configure BIG-IP® GTM™ to acquire information about the health of a third-party server using SNMP, perform the following tasks.

Creating an SNMP monitor

Defining a third-party host server that is running SNMP

Creating an SNMP monitor

Create an SNMP monitor that GTM™ can use to monitor a third-party server running SNMP.

1. On the Main tab, click **DNS** > **GSLB** > **Monitors**.
   The Monitor List screen opens.
2. Click **Create**.
   The New Monitor screen opens.
3. Type a name for the monitor.

   Important: *Monitor names are limited to 63 characters.*

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

Defining a third-party host server that is running SNMP

Ensure that the third-party host server is running SNMP. During this procedure, you assign a virtual server to the server; therefore, determine the IP address that you want to assign to the virtual server.

On the BIG-IP® GTM™, define a third-party host server that is the ultimate destination of DNS queries.

1. On the Main tab, click **DNS** > **GSLB** > **Servers**.
   The Server List screen opens.
2. Click **Create**.
   The New Server screen opens.
3. In the **Name** field, type a name for the server.

   Important: *Server names are limited to 63 characters.*

4. From the **Product** list, select a third-party host server or select **Generic Host**.
   The server type determines the metrics that the system can collect from the server.
5. In the Address List area, add the IP addresses of the server.
   a) Type an external (public) IP address in the **Address** field, and then click **Add**.

b) If you use NAT, type an internal (private) IP address in the **Translation** field, and then click **Add**.

You can add more than one IP address, depending on how the server interacts with the rest of your network.

6. From the **Data Center** list, select the data center where the server resides.
7. From the **Prober Pool** list, select one of the following.

Option	Description
Inherit from Data Center	By default, a server inherits the Prober pool assigned to the data center in which the server resides.
Prober pool name	Select the Prober pool that contains the BIG-IP systems that you want to perform monitor probes of this server.

8. In the Health Monitors area, assign an SNMP monitor to the server by moving it from the **Available** list to the **Selected** list.
9. From the **Virtual Server Discovery** list, select **Disabled**.
10. In the Virtual Server List area, if you selected **Disabled** from the **Virtual Server Discovery** list, create a virtual server to represent (in a pool) the host server that you are creating.
    a) In the **Name** field, type a name for the virtual server.
    b) In the **Address** field, type the IP address of the host server.
    c) From the **Service Port** list, select **SNMP**.
    d) Click **Add**.
11. Click **Create**.
    The Server List screen opens displaying the new server in the list.

Implementation result

BIG-IP® GTM™ can now use the SNMP monitor to verify the availability of and to collect statistics about the generic host.

Chapter 19

Troubleshooting a BIG-IP System with a Rate-Limited License

- *About GTM and DNS rate-limited license statistics*

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.*

Chapter 20

How to Diagnose Network Connection Issues

- *Diagnosing network connection issues*

Diagnosing network connection issues

To help you diagnose network connection issues, you can view the status of and statistics about the iQuery® connections between BIG-IP® Global Traffic Manager™ (GTM) and other BIG-IP systems on your network. iQuery connection information displays for IP addresses that are configured on BIG-IP server objects.

Viewing iQuery statistics

Ensure that the BIG-IP® GTM™ configuration contains at least one BIG-IP server object with a self IP address.

To view information about the connections between BIG-IP GTM and other BIG-IP systems, view iQuery® statistics.

1. On the Main tab, click **Statistics** > **Module Statistics** > **DNS** > **GSLB**.
   The Global Traffic statistics screen opens.
2. From the **Statistics Type** list, select **iQuery**.
   Information about the iQuery connections between this system and other BIG-IP systems in your network displays.
3. When you want to estimate iQuery traffic throughput, click **Reset**.
   The following statistics are reset to zero:
   - iQuery Reconnects
   - Bytes In
   - Bytes Out
   - Backlogs
   - Bytes Dropped

To view information about the iQuery® connections between a different BIG-IP GTM and the BIG-IP systems in your network, log in to that BIG-IP GTM and repeat this procedure.

iQuery statistics descriptions

The information in the table describes the iQuery® statistics.

iQuery Statistics	Description
IP Address	Displays the IP addresses of the servers that have an iQuery connection with this BIG-IP®GTM™.
Server	Displays the name of the server with the specified IP address.
Data Center	Displays the data center to which the specified server belongs.
iQuery State	Displays the state of the iQuery connection between the specified server and the GTM. Possible states are: • Not Connected • Connecting

iQuery Statistics	Description
	• Connected • Backlogged (indicates messages are queued and waiting to be sent)
iQuery Reconnects	Displays the number of times the GTM re-established an iQuery connection with the specified server.
Bytes In	Displays the amount of data in bytes received by the GTM over the iQuery connection from the specified server.
Bytes Out	Displays the amount of data in bytes sent from the GTM over the iQuery connection to the specified server.
Backlogs	Displays the number of times the iQuery connection between the GTM and the specified server was blocked, because iQuery had to send out more messages than the connection could handle.
Bytes Dropped	Displays the amount of data in bytes that the iQuery connection dropped.
SSL Certificate Expiration	Displays the date the SSL certificate expires.
Configuration Time	Displays the date and time that the GTM configuration was last modified. The timestamps should be the same for all devices in a GTM synchronization group.

Index

A

allow-transfer statement
    modifying for zone transfers *43*
APN
    and listeners *59*
    and wide IPs *61*
authentication
    and SSL certificate chains *86*
    and SSL certificates *82*
authoritative name server, designating GTM *44*
authorizing BIG-IP communications *16*
auto-discovery, disabling at the global-level *73*
automatic configuration save
    changing the save interval *101*
    disabling *100*
    disabling using tmsh *101*
automatic configuration save timeout
    changing *100*
automatic save
    about *100*
    configuring the save timeout *100*
auto-save
    configuring the save timeout *100*

B

big3d_install script, running *19*
big3d agent
    and iQuery *16*
    and SSL certificates *82*
    importing certificate chains *85*
    importing root certificate *83*
    upgrading *19*
bigip_add utility
    and integrating LTM with GTM *22*
    running *25*
BIG-IP communications *16*
BIG-IP LTM
    and route domains *64*
    and server definition *18*, *24*
BIG-IP systems, and iQuery connections *112*
Bridge mode, and global traffic management *49*

C

canonical names
    and pools *38*
canonical names, and creating pools *38*
CA servers, and device certificates *84*
certificate chains
    and SSL authentication *84*
    creating *84*
    verifying exchange *85*
certificate exchange, verifying *83*
certificates
    importing device *82*
certificates, importing device *84*
CNAME record
    and redirecting DNS queries *38*
CNAME records
    about *38*
CNAME resolutions
    viewing statistics about *39*
configuration changes
    and configuring manual save *100*
configuration files, acquiring *30*
configuration saves
    and changing the save timeout *100*
configuration synchronization
    enabling for GTM *78*
connection refused error
    and listeners *45*
    and TCP protocol *45*
connections
    viewing iQuery statistics *112*
    viewing status *112*
custom GTP monitors
    and GTP load balancing *60*
    creating *60*

D

data centers
    assigning Prober pools *96*
    creating *29*
    defining *16*, *22*, *57*, *77*, *94*
delegated zones
    and listeners *35*
    creating on local DNS servers *35*
deterministic probing, implementing *92*
device certificates
    and CA servers *82*
    importing *82*, *84*
disabling automatic configuration save *100*
disabling automatic save *101*
DNS queries
    creating listeners to forward *49*
DNS queries for GTM
    load balancing *20*
DNS server pools, and listeners *53*
DNS servers
    and creating pools *53*
    and GTM *48*
    and pools *52*
    and wide IPs *34*
    configuring to allow zone transfers *43*
    delegating wide IP requests *34*
    identifying legacy *44*
    modifying *44*
    replacing with GTM *42*
DNS Services
    about rate-limited license statistics *110*
DNS statistics
    viewing per wide IP *39*

DNS traffic
and GTM 48
and statistics per wide IP 39
and wide IPs 48
creating listeners to identify 45
forwarding 48
identifying 35
routing 48

E

effective rate limit (RPS)
about rate-limited license statistics 110
enabling automatic save 101
enabling manual save 100

F

file transfers, See zone transfers.
forwarding traffic to DNS servers 48

G

global server load balancing
and decision logs 104
global traffic management
and wildcard listeners 48
load balancing to a pool of DNS servers 52
global traffic management, and Bridge mode 49
GTM
about rate-limited license statistics 110
and bigip_add utility 25
integrating with LTM 22
gtm_add script
and server status 29
running 30
using 79
gtmd agent
and importing root certificates 83
and SSL certificates 82
importing certificate chains 85
gtmd agent, and iQuery 16
GTM synchronization groups
about 28
adding new GTM 28
illustrated 28
GTP load balancing
and custom GTP monitors 60
GTP monitor
and packet gateways 56

H

high-speed remote logs
and load-balancing decisions 104
hosts, defining 106

I

integrating with existing DNS servers 34
integration of GTM with older systems 16
integration of LTM and GTM systems 22
intelligent probing, about 92
iQuery
and big3d agent 16
and gtmd agent 16
and statistics 112
viewing statistics about connections 112
viewing status of connections 112
iQuery connections
and statistics 112
and status 112

L

LDNS, creating delegated zones 35
legacy DNS servers
and zone transfers 43
identifying by self IP addresses on BIG-IP GTM 44
Level 1, about SSL authentication 82
listeners
about wildcard 48
and pools of DNS servers 53
and refused connection error 45
and TCP protocol 45
and UDP protocol 45
creating to forward DNS queries 49
creating to handle wide IP traffic locally 35
creating to identify APNs 59
creating to identify DNS traffic 45, 76
defined 34, 42, 48, 52
load balancing DNS queries for GTM 20
load balancing process
about Prober pool status 93
about traffic management capabilities 16
and non-wide IP traffic 52
and Prober pools 92
load balancing traffic to a pool of DNS servers 52
local DNS servers, and replacing with GTM 42
logging
enabling load-balancing decision logs for a wide IP 104
logical network components
and creating wide IPs 45, 50
logs, and Prober pool data 97
LTM
and bigip_add utility 25
and route domains 64, 70
and server definition 18, 24
integrating with GTM 22

M

manual save
configuring using tmsh 101
enabling 100

N

negative DNS responses, and GTM 88
network, deploying GTM for single route domain 64
network connection issues, diagnosing 112
network placement of GTM forwarding traffic 49

network traffic
listeners *34*, *42*, *48*, *52*
NTP servers, defining *76*

O

object count
about rate-limited license statistics *110*

P

packet gateway
defining *58*
packet gateways
and GTM monitoring *56*
packet gateway systems
and creating a pool *61*
placement of GTM on network to forward traffic *49*
pool
creating for packet gateway systems *61*
pools
and CNAME records *38*
and DNS servers *52–53*
creating *88*
creating with canonical name *38*
primary servers, defining for zones *44*
Prober pools
about *92*
about statistics *93*
about status *93*
and data centers *96*
and deterministic probing *92*
and logs *97*
and servers *96*
and statistics *96*
creating *95*

R

rate-limited DNS Services license
and viewing statistics *110*
rate-limited GTM license
and viewing statistics *110*
rate rejects
about rate-limited license statistics *110*
redirect using CNAME record
about *38*
redundant system configurations
and GTM *76*
defining servers *77*
refused connection error *45*
replacing local DNS servers *42*
rollover, See emergency rollover. *76*
root certificates, importing *83*
root servers, and zones *44*
route domains
and GTM *64*
and LTM *64*, *70*
and self IP addresses *66*, *73*
and server definition *66*, *73*
and VLANs *65*, *72*
creating *65*, *72*
route domains *(continued)*
deploying GTM on network with multiple route domains *70*
routing traffic to DNS servers *48*

S

saving configuration changes
about *100*
and changing the save interval using tmsh *101*
and changing the save timeout *100*
and configuring manual save *100*
scripts
running big3d_install script *19*
running gtm_add script *29*
self IP addresses
and route domains *73*
creating for route domains *66*
creating on GTM for legacy DNS servers *44*
self-signed SSL certificates, about *82*
server
creating *94*
server pools, and listeners *53*
servers
assigning Prober pools *96*
defining BIG-IP LTM systems *18*, *24*
defining for BIG-IP GTM *17*, *22*, *57*
defining for route domains *66*, *73*
defining GTM redundant system configurations *77*
defining new BIG-IP GTM *29*
defining third-party host servers *106*
single route domain, deploying GTM on network *64*
SNMP monitoring
and third-party host servers *106*
creating monitors *106*
SOA records
about *88*
and wide IPs *88*
SSL authentication
about *82*
and certificate chains *86*
defined *82*
SSL certificates
about Level 1 SSL authentication *82*
about self-signed *82*
and big3d agent *83*, *85*
and CA servers *82*
and certificate chain authentication *84*
and gtmd agent *83*, *85*
and verifying chain exchange *85*
creating chains *84*
signed by third party *82*
verifying exchange *83*
statistics
about iQuery *112*
viewing for DNS traffic per wide IP *39*
viewing for Prober pools *96*
viewing per wide IP *39*
statistics, and Prober pools *93*
status, and Prober pools *93*
synchronization
enabling *28*

synchronization *(continued)*
enabling for GTM *78*
synchronization groups
about *28*
adding new GTM *28*
illustrated *28*

T

TCP protocol
and connection refused error *45*
and listeners *45*
third-party servers, and SNMP monitoring *106*
traffic forwarding, placement of GTM *49*

U

UDP protocol, and listeners *45*

V

virtual servers
disabling auto-discovery at the global-level *73*
VLANs
creating for a route domain on BIG-IP LTM *72*
creating for route domains *65*

W

wide IPs
and DNS servers *34*, *48*
and DNS traffic *35*
and load-balancing decision logs *104*
and pools configured with a CNAME *38*
and SOA records *88*
configuring for an APN *61*
creating *45*, *50*
enabling load-balancing decision logging *104*
wildcard listeners, defined *48*

Z

zones
and GTM as primary server *44*
and root servers *44*
zone transfers
and configuring DNS servers *43*
and legacy DNS servers *43*