BIG-IP® DNS: Implementations

Version 12.1

Table of Contents

Table of Contents

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

Overview: Integrating BIG-IP DNS (formerly GTM) with other BIG-IP systems on a network

You can add BIG-IP® DNS 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 BIG-IP DNS devices in a BIG-IP DNS synchronization group, and the LTM and Link Controller devices that are configured to communicate with the devices in the BIG-IP DNS 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® DNS 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.
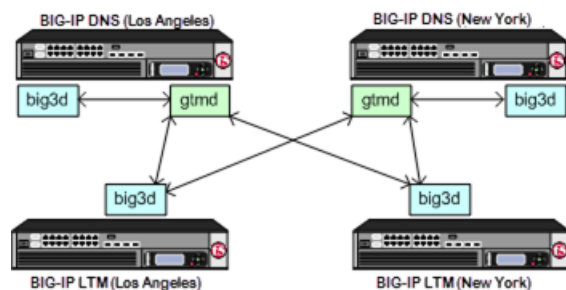
Figure 1: Communications between big3d and gtmd agents using iQuery

Task summary

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

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

Defining a data center

On BIG-IP®DNS, 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 DNS systems

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

On BIG-IP® DNS, create a server object to represent the BIG-IP DNS 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**.
5. In the Address List area, add the non-floating 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 BIG-IP DNS system or for a BIG-IP DNS/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 BIG-IP DNS/LTM combo system when you want the BIG-IP DNS 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 BIG-IP DNS/LTM combo system when you want the BIG-IP DNS 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 BIG-IP DNS system or for a BIG-IP DNS/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 BIG-IP DNS/LTM combo system when you want BIG-IP DNS 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 BIG-IP DNS/LTM combo system when you want BIG-IP DNS to discover links.

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

Defining BIG-IP LTM systems

On DNS, 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 **BIG-IP System**.

5. In the Address List area, add the non-floating 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 BIG-IP DNS system or for a BIG-IP DNS/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 BIG-IP DNS/LTM combo system when you want the BIG-IP DNS 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 BIG-IP DNS/LTM combo system when you want the BIG-IP DNS 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 BIG-IP DNS system or for a BIG-IP DNS/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 BIG-IP DNS/LTM combo system when you want BIG-IP DNS 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 BIG-IP DNS/LTM combo system when you want BIG-IP DNS 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 DNS 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 SOL1332 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 DNS 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 BIG-IP DNS 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 BIG-IP DNS 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. DNS 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.

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

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

You can add BIG-IP® Local Traffic Manager™ (LTM®) systems to a network in which BIG-IP® DNS (formerly 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 BIG-IP DNS systems. When the LTM and BIG-IP DNS 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 DNS 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 DNS and BIG-IP LTM systems, perform the following tasks on BIG-IP DNS.
Defining a data center
Defining BIG-IP DNS systems
Defining BIG-IP LTM systems
Running the bigip_add script

Defining a data center

On BIG-IP®DNS, 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 DNS systems

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

On BIG-IP® DNS, create a server object to represent the BIG-IP DNS 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**.
5. In the Address List area, add the non-floating 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 BIG-IP DNS system or for a BIG-IP DNS/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 BIG-IP DNS/LTM combo system when you want the BIG-IP DNS 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 BIG-IP DNS/LTM combo system when you want the BIG-IP DNS 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 BIG-IP DNS system or for a BIG-IP DNS/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 BIG-IP DNS/LTM combo system when you want BIG-IP DNS 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 BIG-IP DNS/LTM combo system when you want BIG-IP DNS to discover links.

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

Defining BIG-IP LTM systems

On DNS, 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 **BIG-IP System**.
5. In the Address List area, add the non-floating 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 BIG-IP DNS system or for a BIG-IP DNS/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 BIG-IP DNS/LTM combo system when you want the BIG-IP DNS system to discover LTM virtual servers.

Option	Description
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 BIG-IP DNS/LTM combo system when you want the BIG-IP DNS 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 BIG-IP DNS system or for a BIG-IP DNS/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 BIG-IP DNS/LTM combo system when you want BIG-IP DNS 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 BIG-IP DNS/LTM combo system when you want BIG-IP DNS 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 DNS.

Run the `bigip_add` script on the BIG-IP DNS 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. For additional information about running the script, see SOL13312 on AskF5.com (`www.askf5.com`).

*Note: The BIG-IP DNS and BIG-IP LTM systems must have TCP port **22** open for the script to work. You must perform this task from the command-line interface.*

1. Log in as `root` to the BIG-IP DNS 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 BIG-IP DNS.

Implementation result

You now have an implementation in which the BIG-IP® systems can communicate with each other. BIG-IP DNS 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.

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

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

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

Configuration changes to one device in a BIG-IP DNS synchronization group are synchronized incrementally across the devices in the group. That is, only the data that has changed on a BIG-IP DNS 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.
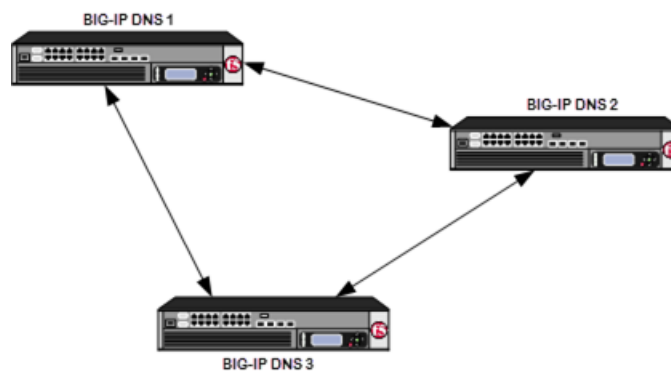
Figure 2: BIG-IP DNS systems in a BIG-IP DNS synchronization group

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

Task summary
When adding BIG-IP® DNS to a network that already contains BIG-IP DNS systems in a synchronization group, perform the following tasks.
Enabling synchronization on the existing BIG-IP DNS
Creating a data center on the existing BIG-IP DNS
Defining a server on the existing BIG-IP DNS
Running the gtm_add script

Enabling synchronization on the existing BIG-IP DNS

Ensure that BIG-IP® DNS references your NTP servers.

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

Enable synchronization on the system to ensure that the BIG-IP DNS system that is already installed on your network can share configuration changes with other BIG-IP DNS systems that you add to the BIG-IP DNS 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 BIG-IP DNS system in the BIG-IP DNS synchronization group, that change is automatically synchronized to the other systems in the group.

Creating a data center on the existing BIG-IP DNS

Create a data center on the existing DNS system to represent the location where the new BIG-IP DNS 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 BIG-IP DNS

Ensure that a data center where the new DNS system resides is available in the configuration of the existing BIG-IP DNS.

Define a new server, on the existing BIG-IP DNS system, to represent the new BIG-IP DNS 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**.
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 BIG-IP DNS system or for a BIG-IP DNS/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 BIG-IP DNS/LTM combo system when you want the BIG-IP DNS 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 BIG-IP DNS/LTM combo system when you want the BIG-IP DNS 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**.

    Note: The gtmd *process on each BIG-IP DNS system will attempt to establish an iQuery® connection over port* 4353 *with each self IP address defined on each server in the BIG-IP DNS configuration of type BIG-IP. Allow port* 4353 *in your port lockdown settings for iQuery® to work.*

    The Server List screen opens displaying the new server in the list.

The status of the newly defined BIG-IP DNS 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 DNS system in the BIG-IP DNS synchronization group to which you want to add another BIG-IP DNS.

Run the gtm_add script on the BIG-IP DNS system you are adding to your network to acquire the configuration settings from a BIG-IP DNS system that is already installed on your network. For additional information about running the script, see SOL13312 on AskF5.com (www.askf5.com).

---

*Note: The BIG-IP DNS and other BIG-IP systems must have TCP port **22** open between the systems for the script to work. You must perform this task from the command-line interface.*

---

1. Log in as root to the BIG-IP DNS 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 BIG-IP DNS system in the synchronization group to which you are adding this BIG-IP DNS system.
   c) Press Enter.
   d) If prompted, type the root password.
   e) Press Enter.

The BIG-IP DNS system you are installing on your network acquires the configuration of the BIG-IP DNS system already installed on your network.

Implementation result

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

Delegating DNS Traffic to BIG-IP DNS

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

BIG-IP® DNS resolves DNS queries that match a wide IP name. BIG-IP DNS 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 DNS for name resolution.
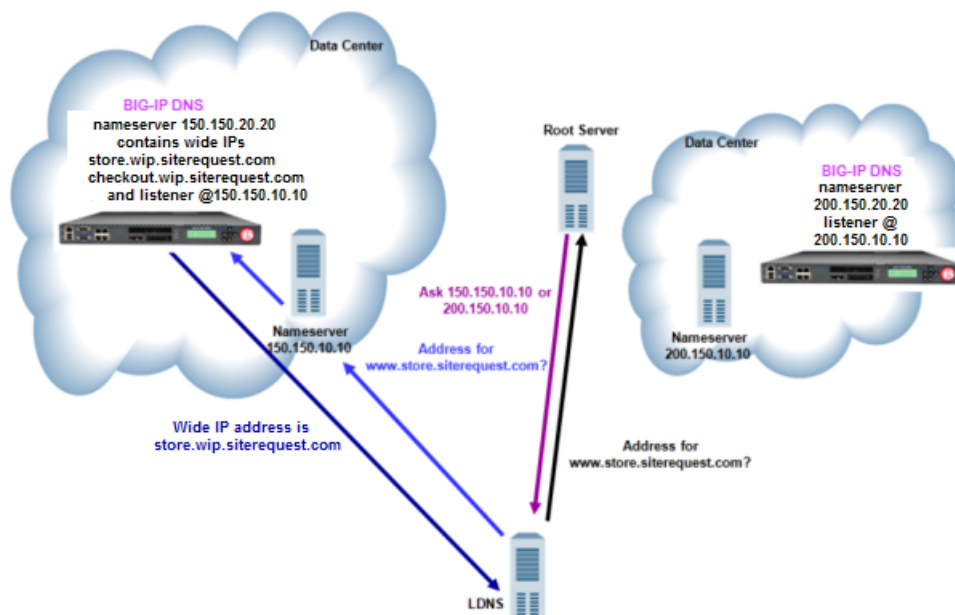
Figure 3: Traffic flow when DNS server delegates traffic to BIG-IP DNS

This implementation focuses on the fictional company SiteRequest that recently purchased BIG-IP DNS 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 DNS with two wide IPs, `store.wip.siterequest.com` and `checkout.wip.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 DNS 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 DNS.

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® DNS.

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 BIG-IP DNS 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 BIG-IP DNS in your network.
2. Create a *nameserver record* (NS record) that defines the delegated zone for which BIG-IP DNS is responsible.
3. Create *canonical name* records (CNAME records) for each web application, which forwards requests to `store.siterequest.com` and `checkout.siterequest.com` to the wide IP addresses of `store.wip.siterequest.com` and `checkout.wip.siterequest.com`, respectively.

Creating listeners to handle traffic for wide IPs

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

Create listeners that identify the wide IP traffic for which BIG-IP DNS 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 BIG-IP DNS listens for network traffic.
   The destination is a self IP address on BIG-IP DNS.
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® DNS 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 DNS, which then load balances the queries to the appropriate wide IPs.

Redirecting DNS Queries Using a CNAME Pool

Overview: Redirecting DNS queries using a CNAME pool

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 type to the wide IP with an A record type 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 CNAME pool with members specifying the canonical name, BIG-IP® DNS responds to DNS name resolution requests for A or CNAME name record type queries with these names if this pool is added to the said wide IP.

Task summary

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

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

Creating a CNAME pool

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

1. On the Main tab, click **DNS** > **GSLB** > **Pools**.
   The Pool 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 **Type** list, select the **CNAME** type.

5. In the Members area, for the **Member List** setting, from the **Wide IP** list, select either a pool member (A or AAAA type) or a static target, and then click **Add**.

6. Click **Finished**.

Creating a wide IP with a CNAME pool

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

Create a wide IP that includes a pool configured with a CNAME to redirect DNS queries from 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**.

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 **Type** list, select a record type to serve from the required DNS query types.

   Note: If you want the BIG-IP®DNS to respond to both A and CNAME record type requests, you must configure two wide IPs. One wide IP of type A with a CNAME pool type, and a second wide IP of type CNAME with a CNAME pool type. At a minimum, an A record type wide IP should be configured with a CNAME pool.

5. In the Pools area, for the **Pool List** setting, from the **Pool** list, select the name of the CNAME pool, and then click **Add**.

6. 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 BIG-IP® DNS (formerly 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® DNS resolves a DNS query for a wide IP to a CNAME.

Replacing a DNS Server with BIG-IP DNS

Overview: Replacing a DNS server with BIG-IP DNS

BIG-IP® DNS load balances incoming wide IP traffic to your network resources. BIG-IP DNS 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 DNS to replace the DNS server that currently manages `www.siterequest.com`. BIG-IP DNS becomes the authoritative nameserver for `www.siterequest.com` and load balances traffic across the web-based applications `store.siterequest.com` and `checkout.siterequest.com`.
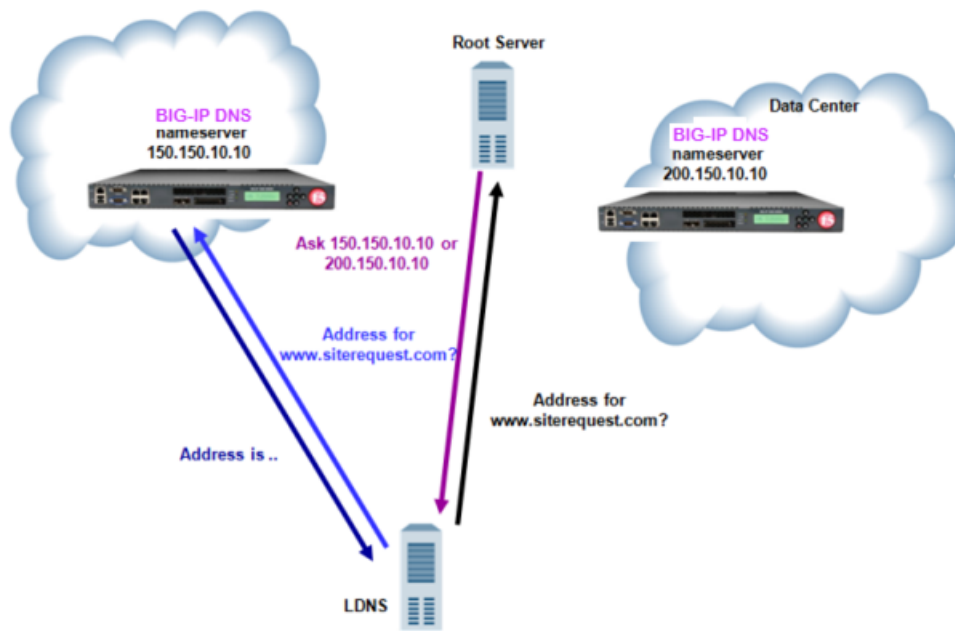
Figure 4: Traffic flow when BIG-IP DNS replaces DNS server

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 DNS 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 DNS.
Configuring BIND servers to allow zone transfers
Performing zone transfers from the legacy DNS server

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® DNS.

In order for BIG-IP DNS 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® DNS from the network.

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

1. On the Main tab, click **Network** > **Self IPs**.

2. Click **Create**.
   The New Self IP screen opens.

3. In the **Name** field, type a unique name for the self IP address.

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.

   For example, you can type `255.255.255.0`.

6. Click **Finished**.
   The screen refreshes, and displays the new self IP address.

Designating BIG-IP DNS as the primary server for the zone

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

Add this self IP address to the BIG-IP DNS 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 BIG-IP DNS 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 DNS. Ensure that the IP address of the DNS server does not conflict with the self IP address that you added to the BIG-IP DNS 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 DNS 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 DNS.

Creating listeners to alert BIG-IP DNS to DNS traffic destined for the system

To alert the BIG-IP® DNS 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 for BIG-IP DNS

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 an 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 List screen opens.
3. In the General Properties area, 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 **Type** list, select a record type for the wide IP.
5. In the Pools area, for the **Pool List** setting, 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**.

6. Click **Finished**.

Implementation result

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

Placing BIG-IP DNS in Front of a DNS Server

Overview: Configuring BIG-IP DNS to screen traffic to an existing DNS server

You can use BIG-IP® DNS as a traffic screener in front of an existing DNS server. With this setup, all DNS traffic flows through BIG-IP DNS. Listeners that you configure on BIG-IP DNS verify incoming DNS queries. If the query is for a wide IP, BIG-IP DNS 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 DNS, the system forwards the query to the specified DNS server for resolution. When forwarding a query, BIG-IP DNS transforms the source address to a self IP address on BIG-IP DNS.
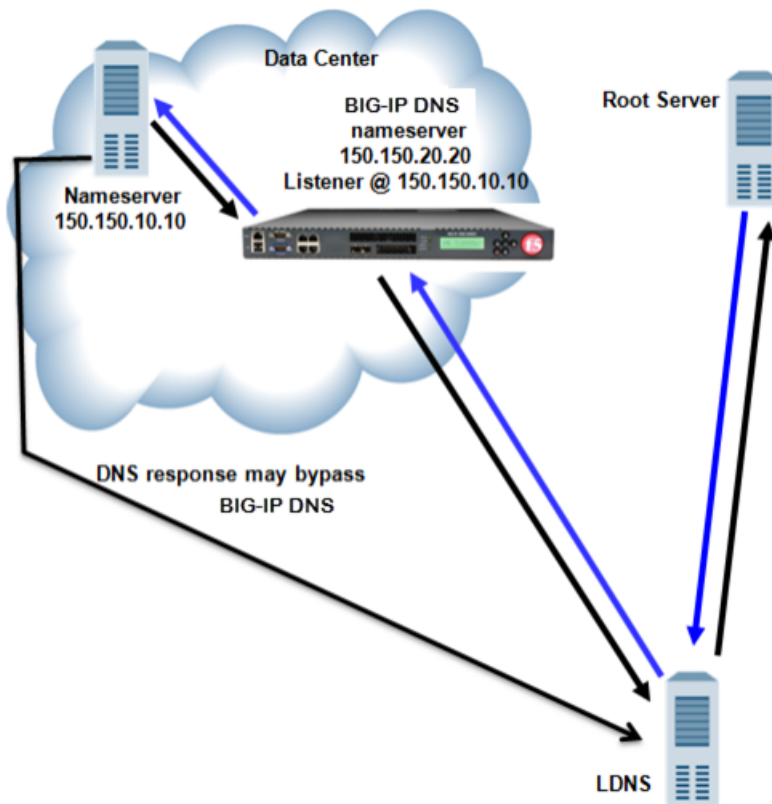
Figure 5: Traffic flow when BIG-IP DNS screens traffic to a DNS server

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

Placing BIG-IP DNS on your network to forward traffic

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

Place BIG-IP DNS on your network between LDNS servers and clients making DNS name resolution requests.

1. Physically connect BIG-IP DNS to your Internet connection.
2. Connect the LDNS to an Ethernet port on BIG-IP DNS (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 BIG-IP DNS 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 BIG-IP DNS.*

   ---

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 for BIG-IP DNS

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 an 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 List screen opens.

3. In the General Properties area, 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 **Type** list, select a record type for the wide IP.

5. In the Pools area, for the **Pool List** setting, 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**.

6. Click **Finished**.

Implementation result

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

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

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

BIG-IP® DNS can function as a traffic screener in front of a pool of DNS servers. In this situation, BIG-IP DNS checks incoming DNS queries and if the query is for a wide IP, resolves the query. Otherwise, BIG-IP DNS forwards the DNS query to one of the servers in a pool of DNS servers, and that server handles the query.
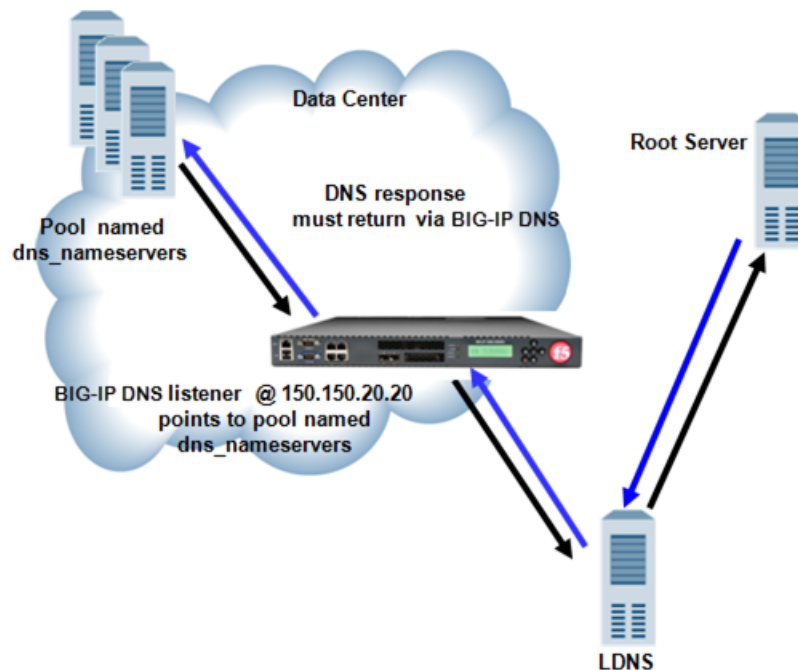
Figure 6: Traffic flow when BIG-IP DNS screens traffic to a pool of DNS servers

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 DNS 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 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 the applicable path.
   - **DNS** > **Delivery** > **Load Balancing** > **Pools**
   - **Local Traffic** > **Pools**

   The Pool List screen opens.
2. Click **Create**.
   The New Pool screen opens.
3. In the **Name** field, type a unique name for the pool.
4. For the **Health Monitors** setting, from the **Available** list, select the custom DNS monitor you created and 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) (Optional) In the **Node Name** field, type a name for the node portion of the pool member.
   b) In the **Address** field, type an IP address.
   c) In the **Service Port** field, type a port number, or select a service name from the list.
   d) (Optional) In the **Priority** field, type a priority number.
   e) Click **Add**.

6. Click **Finished**.

Creating listeners that alert BIG-IP DNS to DNS queries for a pool of DNS servers

Ensure that a pool of DNS servers exists on DNS.

Configure a listener that alerts BIG-IP DNS 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 BIG-IP DNS 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 BIG-IP DNS 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® DNS receives DNS queries, handles wide IP requests, and forwards all other DNS queries to members of the pool of DNS servers.

Configuring BIG-IP DNS to Determine PGW Health and Availability

Overview: Configuring BIG-IP DNS to determine packet gateway health and availability

Service providers can configure the BIG-IP® DNS 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. BIG-IP DNS 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: *BIG-IP DNS 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.
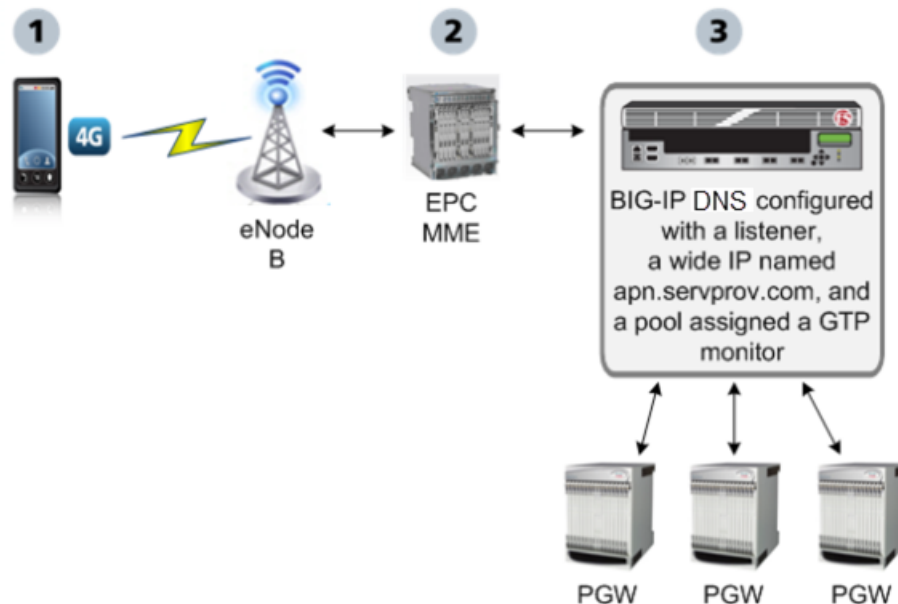
Figure 7: BIG-IP DNS monitoring packet gateways

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. BIG-IP DNS handles the DNS request and returns only IP addresses for PGW systems that are active and available.

Task summary

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

Defining a data center

Defining BIG-IP DNS 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 with an applicable pool type

Configuring a wide IP for load balancing APN lookups

Defining a data center

On BIG-IP®DNS, 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 DNS systems

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

On BIG-IP® DNS, create a server object to represent the BIG-IP DNS 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**.

5. In the Address List area, add the non-floating 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 BIG-IP DNS system or for a BIG-IP DNS/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 BIG-IP DNS/LTM combo system when you want the BIG-IP DNS 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 BIG-IP DNS/LTM combo system when you want the BIG-IP DNS 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 BIG-IP DNS system or for a BIG-IP DNS/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 BIG-IP DNS/LTM combo system when you want BIG-IP DNS 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 BIG-IP DNS/LTM combo system when you want BIG-IP DNS 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® DNS system that you are configuring.

Define the PGW systems to which BIG-IP DNS 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® DNS 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 BIG-IP DNS 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 Monitor** 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 with an applicable pool type

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 or wide IP to each server.
- Create a GTP monitor.

You can create a pool of packet gateway systems with an applicable pool type to which the BIG-IP® system can load balance global traffic.

Creating a pool with pool type A or AAAA

Create an A or AAAA pool type in order to configure the BIG-IP® system to load balance global traffic.

1. On the Main tab, click **DNS** > **GSLB** > **Pools**.
The Pool List screen opens.

2. Click **Create**.

3. In the General Properties area, 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 **Type** list, depending on the type of the system (IPv4 or IPv6), select either an **A** or **AAAA** pool type.

5. In the Configuration area, for the **Health Monitors** setting, in the **Available** list, select a monitor type, and move the monitor to the **Selected** list.

Tip: Hold the Shift or Ctrl key to select more than one monitor at a time.

6. In the Members area, for the **Load Balancing Method** setting, from the **Preferred List**, select **Round Robin**.

Note: When you create a pool of one or more packet gateway systems (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.

*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.*

7. 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.

8. In the Members area, 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**.

9. Click **Finished**.

Creating a pool with pool type NAPTR

Create an NAPTR pool type in order to configure the BIG-IP® system to load balance global traffic.

1. On the Main tab, click **DNS** > **GSLB** > **Pools**.
   The Pool List screen opens.

2. Click **Create**.

3. In the General Properties area, 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 **Type** list, select the **NAPTR** type.

5. In the Members area, for the **Load Balancing Method** setting, from the **Preferred List**, select **Round Robin**.

   Note: When you create a pool of one or more packet gateway systems (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.

   ---

   *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. 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. In the Members area, for the **Member List** setting, from the **Flags** list, select a flag.

8. Add wide IPs as members of this load balancing pool.

   The system evaluates the wide IPs (pool members) in the order in which they are listed. A wide IP can belong to more than one pool.

   a) From the **Wide IP** list, select a wide IP or type a name that matches an existing wildcard wide IP.
   b) In the **Service** field, type the name of a service or protocol.
   c) Click **Add**.

9. Click **Finished**.

Creating a pool with pool type SRV

Create a SRV pool type in order to configure the BIG-IP® system to load balance global traffic.

1. On the Main tab, click **DNS** > **GSLB** > **Pools**.
   The Pool List screen opens.
2. Click **Create**.
3. In the General Properties area, 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 **Type** list, select the **SRV** type.
5. In the Members area, for the **Load Balancing Method** setting, from the **Preferred List**, select **Round Robin**.

   Note: When you create a pool of one or more packet gateway systems (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.

   *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. 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. In the Members area, for the **Member List** setting, from the **Flags** list, select a flag.
8. Add wide IPs as members of this load balancing pool.

   The system evaluates the wide IPs (pool members) in the order in which they are listed. A wide IP can belong to more than one pool.

   a) From the **Wide IP** list, select a wide IP or type a name that matches an existing wildcard wide IP.
   b) In the **Service** field, type the name of a service or protocol.
   c) Click **Add**.

9. Click **Finished**.

Creating a pool with pool type CNAME

1. On the Main tab, click **DNS** > **GSLB** > **Pools**.
   The Pool List screen opens.
2. Click **Create**.
3. In the General Properties area, 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 **Type** list, select the **CNAME** type.

5. In the Members area, for the **Load Balancing Method** setting, from the **Preferred List**, select **Round Robin**.

Note: When you create a pool of one or more packet gateway systems (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.

*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. 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. Add wide IPs as members of this load balancing pool.

The system evaluates the wide IPs (pool members) in the order in which they are listed. A wide IP can belong to more than one pool.

a) In the Members area, for the **Member** setting, from the **Wide IP** list, select a wide IP or type a name that matches either an existing wildcard wide IP or wide IP alias.

b) If necessary, to allow the member to point to a name that does not exist as a wide IP on DNS, select the **Static Target** check box.

c) Click **Add**.

8. Click **Finished**.

Creating a pool with pool type MX

Create a MX pool type in order to configure the BIG-IP® system to load balance global traffic.

1. On the Main tab, click **DNS** > **GSLB** > **Pools**.
The Pool List screen opens.

2. Click **Create**.

3. In the General Properties area, 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 **Type** list, select the **MX** type.

5. In the Members area, for the **Load Balancing Method** setting, from the **Preferred List**, select **Round Robin**.

Note: When you create a pool of one or more packet gateway systems (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.

*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. 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. Add wide IPs as members of this load balancing pool.

   The system evaluates the wide IPs (pool members) in the order in which they are listed. A wide IP can belong to more than one pool.

   a) In the Members area, for the **Member** setting, from the **Wide IP** list, select a wide IP or type a name that matches an existing wildcard wide IP.

   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® DNS 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 List screen opens.

3. In the General Properties area, in the **Name** field, type the APN, for example `apn.servprov.com`.

4. From the **Type** list, select one of these record types for the wide IP:

Option	Description
NAPTR	The Name Authority Pointer record, NAPTR, aids in the standardization of Uniform Resource Names (URNs). NAPTR records map between sets of URNs, URLs and plain domain names, and suggest to clients the protocols available for communication with the mapped resource.
A	The Address record, or A record, lists the IP address for a given host name.
SRV	The Service resource record, SRV, is a pointer with which an alias for a given service is redirected to another domain.
CNAME	The Canonical Name resource record, CNAME, specifies an alias or nickname for the official, or canonical, host name.
AAAA	The IPv6 Address record, or AAAA record, lists the 128-bit IPv6 address for a given host name.
MX	The Mail Exchange resource record, MX, defines the mail system(s) for a given domain.

5. In the Pools area, from the **Load Balancing Method** list, select **Round Robin**.

6. From the **Pool** list, select the pool of PGW systems, and then click **Add**.

7. Click **Finished**.

Configuring BIG-IP DNS on a Network with One Route Domain

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

You can deploy BIG-IP® DNS 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 BIG-IP DNS, you can configure route domains on internal interfaces only. F5 Networks does not support the configuration of route domains on a standalone BIG-IP DNS.*
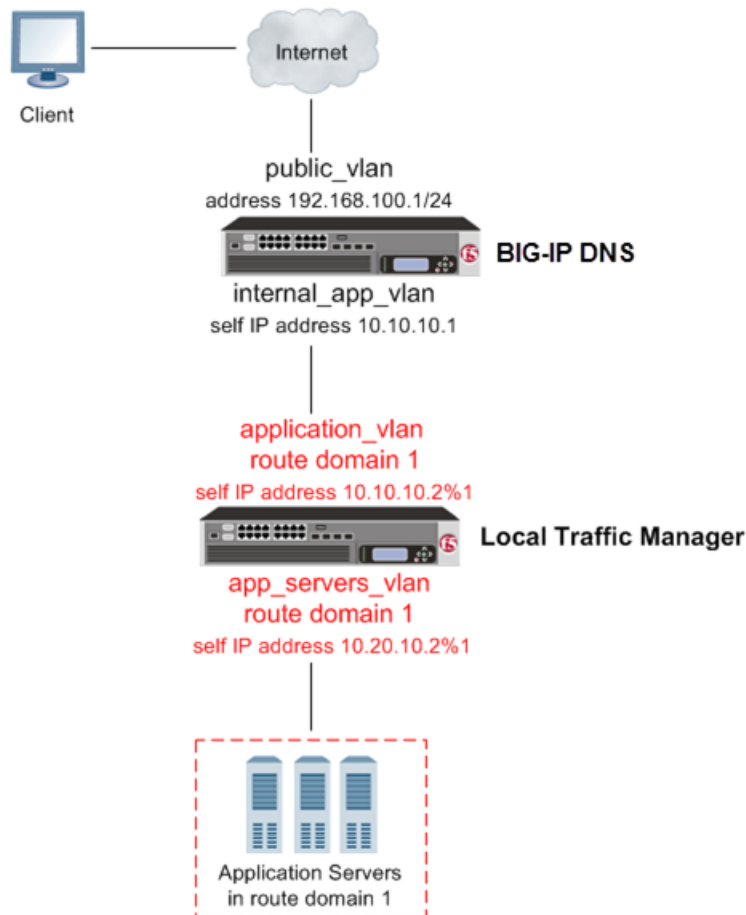

Figure 8: BIG-IP DNS deployed on a network in front of a BIG-IP LTM configured with a route domain

Task summary

Perform these tasks to configure a route domain, and then to configure BIG-IP DNS to be able to monitor the LTM systems.

Creating VLANs for a route domain on BIG-IP LTM

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, between 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:
   a) From the **Interface** list, select an interface number or trunk name.
   b) From the **Tagging** list, select **Tagged** or **Untagged**.

      Select **Tagged** when you want traffic for that interface to be tagged with a VLAN ID.

   c) If you specified a numeric value for the **Customer Tag** setting and from the **Tagging** list you selected **Tagged**, then from the **Tag Mode** list, select a value.
   d) Click **Add**.
   e) Repeat these steps for each interface or trunk that you want to assign to the VLAN.

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 in 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.

   An example of a route domain ID is 1.

5. In the **Description** field, type a description of the route domain.
   For example: This route domain applies to application traffic for Customer A.

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.

   Important: *You must enable the BGP protocol.*

   ---

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**.
2. Click **Create**.
   The New Self IP screen opens.
3. In the **Name** field, type a unique name for the self IP address.
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.

   For example, you can type `255.255.255.0`.

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 DNS

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

On a BIG-IP® DNS 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 **BIG-IP System**.

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® DNS can monitor virtual servers on BIG-IP LTM® systems configured with one route domain.

Configuring BIG-IP DNS on a Network with Multiple Route Domains

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

You can deploy BIG-IP® DNS (formerly 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 BIG-IP® system that includes both Local Traffic Manager™ (LTM®) and Global Traffic Manager™ (now BIG-IP® DNS), all IP addresses that BIG-IP DNS references (virtual IP addresses, link addresses, and so on) must be associated with route domain `0`.

The following figure shows BIG-IP DNS deployed in a network with multiple BIG-IP Local Traffic Manager™ (LTM®) systems, one configured with the default route domain (zero), and one configured with two additional route domains. BIG-IP DNS 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 DNS 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.
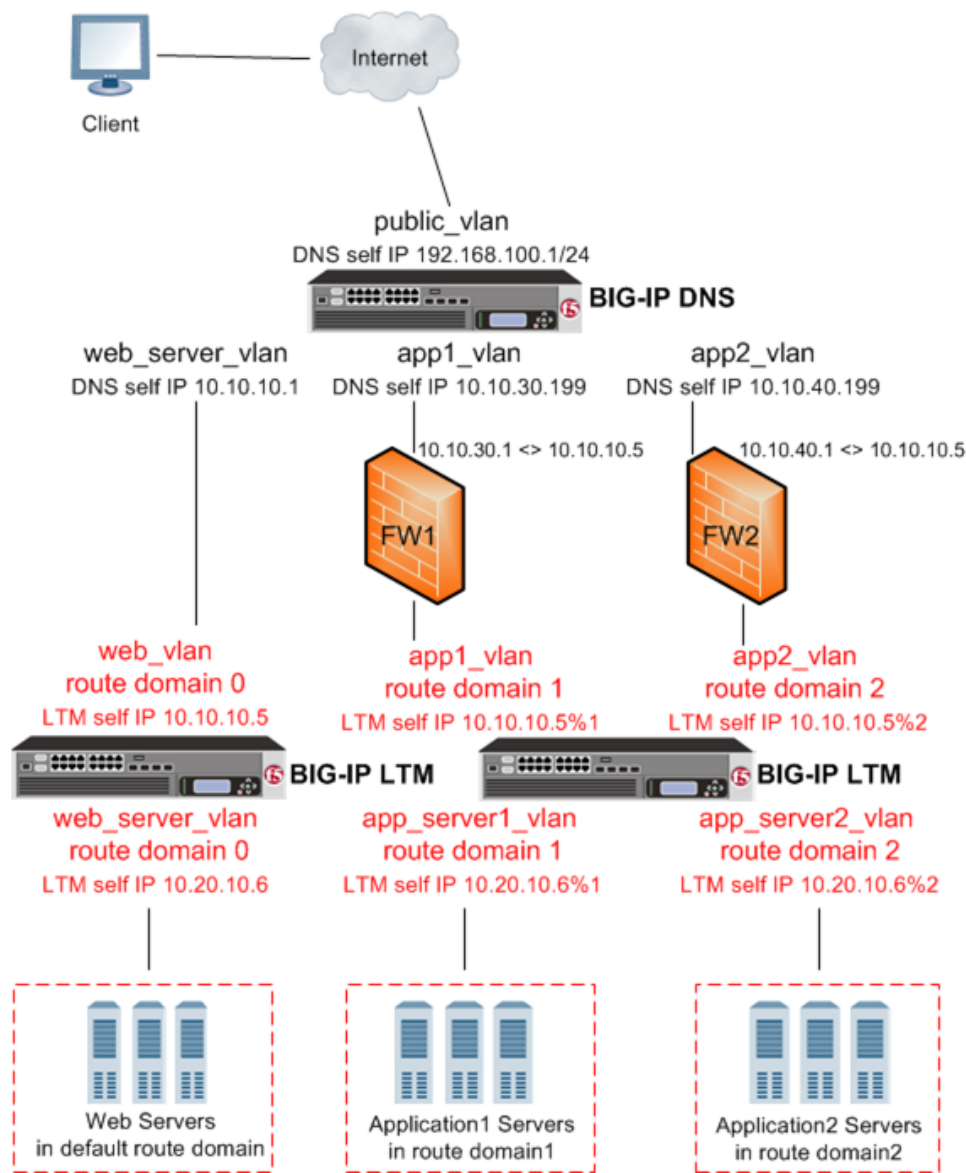
Figure 9: BIG-IP DNS deployed on a network with multiple route domains

Before BIG-IP® DNS can gather status and statistics for the virtual servers hosted on BIG-IP LTM® systems 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, configure a BIG-IP DNS server object on BIG-IP DNS to represent each LTM system device.

Task summary

Perform the following tasks to configure BIG-IP DNS 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

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

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, between 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. If you want to use Q-in-Q (double) tagging, use the **Customer Tag** setting to perform the following two steps. If you do not see the **Customer Tag** setting, your hardware platform does not support Q-in-Q tagging and you can skip this step.

   a) From the **Customer Tag** list, select **Specify**.

   b) Type a numeric tag, from 1-4094, for the VLAN.

   The customer tag specifies the inner tag of any frame passing through the VLAN.

6. For the **Interfaces** setting:

   a) From the **Interface** list, select an interface number or trunk name.

   b) From the **Tagging** list, select **Tagged** or **Untagged**.

   Select **Tagged** when you want traffic for that interface to be tagged with a VLAN ID.

   c) If you specified a numeric value for the **Customer Tag** setting and from the **Tagging** list you selected **Tagged**, then from the **Tag Mode** list, select a value.

   d) Click **Add**.

   e) Repeat these steps for each interface or trunk that you want to assign to the VLAN.

7. 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.

8. Click **Finished**.
   The screen refreshes, and displays the new VLAN in 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.

An example of a route domain ID is 1.

4. In the **Description** field, type a description of the route domain.
   For example: `This route domain applies to application traffic for Customer A.`

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**.

2. Click **Create**.
   The New Self IP screen opens.

3. In the **Name** field, type a unique name for the self IP address.

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.

   For example, you can type `255.255.255.0`.

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.

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

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

On BIG-IP® DNS, define a server object to represent each LTM system device.

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**.

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 Preference** list, select one of the following.

Option	Description
Inside the Data Center	By default, a server selects the Prober pool from within the existing data center.
Outside the Data Center	A server selects the Prober pool from outside the existing data center.
Inherit from Data Center	A server inherits the Prober pool assigned to the data center in which the server resides.

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

   ---

8. From the **Prober Fallback** list, select one of the following.

Option	Description
Any available	By default, selects any available Prober pool.
Inside the Data Center	A server selects the Prober pool from within the existing data center.
Outside the Data Center	A server selects the Prober pool from outside the existing data center.
Inherit from Data Center	A server inherits the Prober pool assigned to the data center in which the server resides.
None	No Prober pool is used. Prober Fallback is disabled.

9. In the Health Monitors area, assign the **bigip** monitor to the server by moving it from the **Available** list to the **Selected** list.

10. From the **Virtual Server Discovery** list, select **Enabled**.

11. Click **Create**.
    The New Server screen opens.

12. In the server list, click the name of the LTM system that you just created.
    The Server Properties screen opens.

13. On the menu bar, click **Virtual Servers**.
    A list of the virtual servers configured on the server displays.

14. From the **Resources** list, select **Advanced**.
Additional settings display.

15. Select the **Expose Route Domains** check box.

16. Click **Update**.

Repeat these steps to create a BIG-IP DNS server object to represent another LTM system device.

Implementation result

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

Setting Up a BIG-IP DNS Redundant System Configuration

Overview: Configuring a BIG-IP DNS redundant system

You can configure BIG-IP® DNS in a redundant system configuration, which is a set of two BIG-IP DNS 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 DNS 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® DNS 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. For the **Time Server Lookup List** setting, 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. For the **Time Server List** setting, in the **Address** field, type the IP address of the NTP server that you want to add. Then click **Add**.
   For this example, type `192.168.5.15`.

   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.

4. For the **Time Server List** setting, in the **Address** field, type the IP address of an NTP server that you want to add. Then click **Add**.

---

*Note: If you are using Dynamic Host Configuration Protocol (DHCP) to assign IP addresses, then the BIG-IP system automatically populates the **Address** field with the fully-qualified domain name (FQDN) of the NTP server.*

---

5. Repeat the preceding step as needed.
6. Click **Update**.

During configuration synchronization, the systems use this time value to determine if any newer configuration files exist.

Creating listeners to identify DNS traffic

Create listeners to identify the DNS traffic that BIG-IP® DNS 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 BIG-IP DNS 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 BIG-IP DNS 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®DNS, 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® DNS 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**.

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 BIG-IP DNS 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 age difference in seconds, between the sets of configuration files on the systems in a BIG-IP DNS configuration synchronization group.

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® DNS 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 BIG-IP DNS 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 BIG-IP DNS systems.

Authenticating with SSL Certificates Signed by a Third Party

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 DNS 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 signed by a CA server
Importing the root certificate for the gtmd agent
Importing the root certificate for the big3d agent
Verifying the certificate exchange

Importing the device certificate signed by a CA server

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® DNS system in the BIG-IP DNS 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® DNS in a BIG-IP DNS 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 running the following commands on all the systems you configure for certificate chain SSL authentication.

```
iqdump <IP address of BIG-IP system 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`).

Configuring a TTL in a DNS NoError Response

Overview: Configuring a TTL in a DNS NoError Response

You can configure BIG-IP® DNS to return 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 DNS 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 General Properties area, 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 **Type** list, depending on the type of the system (IPv4 or IPv6), select either an **A** or **AAAA** pool type.
5. In the Configuration area, for the **Health Monitors** setting, in the **Available** list, select a monitor type, and move the monitor to the **Selected** list.

Tip: *Hold the Shift or Ctrl key to select more than one monitor at a time.*

---

6. In the Members area, 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**.

7. 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® DNS 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 List 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 **Type** list, select a record type for the wide IP.

Note: *Once created, both the record type and name cannot be changed.*

---

6. From the **NoError Response** list, select **Enabled**.

   With this option enabled, the system responds faster to requests for which it does not have AAAA records configured.

7. In the **NoError TTL** field, type the number of seconds that the local DNS servers consider the NoError response to be valid. When you set this value, you must enable the **NoError Response** setting as well.
8. In the Pools area, for the **Pool List** setting, 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**.

9. Click **Finished**.

Implementation result

You now have an implementation in which BIG-IP® DNS returns a TTL in a DNS NoError response for a web site represented by a wide IP in the DNS configuration.

Configuring a TTL in a Return Code On Failure

Overview: Configuring a SOA Negative Caching TTL in a Return Code on Failure

You can configure BIG-IP® DNS to return a start of authority (SOA) Negative Caching time-to-live (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 Return Code On Failure to a query.

Task summary

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

Creating a pool with an applicable pool type
Creating a wide IP that provides for negative caching

Creating a pool with an applicable pool type

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

Create a pool in order to configure the BIG-IP® system to load balance global traffic.

Creating a pool with pool type A or AAAA

Create an A or AAAA pool type in order to configure the BIG-IP® system to load balance global traffic.

1. On the Main tab, click **DNS** > **GSLB** > **Pools**.
   The Pool List screen opens.
2. Click **Create**.
3. In the General Properties area, 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 **Type** list, depending on the type of the system (IPv4 or IPv6), select either an **A** or **AAAA** pool type.

5. In the Configuration area, for the **Health Monitors** setting, in the **Available** list, select a monitor type, and move the monitor to the **Selected** list.

Tip: Hold the Shift or Ctrl key to select more than one monitor at a time.

---

6. In the Members area, for the **Load Balancing Method** setting, 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.*

---

7. 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.

8. In the Members area, 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**.

9. Click **Finished**.

Creating a pool with pool type NAPTR

Create an NAPTR pool type in order to configure the BIG-IP® system to load balance global traffic.

1. On the Main tab, click **DNS** > **GSLB** > **Pools**.
   The Pool List screen opens.
2. Click **Create**.
3. In the General Properties area, 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 **Type** list, select the **NAPTR** type.
5. In the Members area, for the **Load Balancing Method** setting, 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. 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. In the Members area, for the **Member List** setting, from the **Flags** list, select a flag.

8. Add wide IPs as members of this load balancing pool.

The system evaluates the wide IPs (pool members) in the order in which they are listed. A wide IP can belong to more than one pool.

   a) From the **Wide IP** list, select a wide IP or type a name that matches an existing wildcard wide IP.

   b) In the **Service** field, type the name of a service or protocol.

   c) Click **Add**.

9. Click **Finished**.

Creating a pool with pool type SRV

Create a SRV pool type in order to configure the BIG-IP® system to load balance global traffic.

1. On the Main tab, click **DNS** > **GSLB** > **Pools**.
   The Pool List screen opens.
2. Click **Create**.
3. In the General Properties area, 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 **Type** list, select the **SRV** type.
5. In the Members area, for the **Load Balancing Method** setting, 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. 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. Add wide IPs as members of this load balancing pool.

   The system evaluates the wide IPs (pool members) in the order in which they are listed. A wide IP can belong to more than one pool.

      a) In the Members area, for the **Member** setting, from the **Wide IP** list, select a wide IP or type a name that matches an existing wildcard wide IP.

      b) In the **Port** field, type a port number.

      c) Click **Add**.

8. Click **Finished**.

Creating a pool with pool type CNAME

Create a CNAME pool type in order to configure the BIG-IP® system to load balance global traffic.

1. On the Main tab, click **DNS** > **GSLB** > **Pools**.
   The Pool List screen opens.
2. Click **Create**.
3. In the General Properties area, 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 **Type** list, select the **CNAME** type.
5. In the Members area, for the **Load Balancing Method** setting, 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. 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. Add wide IPs as members of this load balancing pool.

   The system evaluates the wide IPs (pool members) in the order in which they are listed. A wide IP can belong to more than one pool.

   a) In the Members area, for the **Member** setting, from the **Wide IP** list, select a wide IP or type a name that matches either an existing wildcard wide IP or wide IP alias.
   b) If necessary, to allow the member to point to a name that does not exist as a wide IP on DNS, select the **Static Target** check box.
   c) Click **Add**.

8. Click **Finished**.

Creating a pool with pool type MX

Create a MX pool type in order to configure the BIG-IP® system to load balance global traffic.

1. On the Main tab, click **DNS** > **GSLB** > **Pools**.
   The Pool List screen opens.
2. Click **Create**.
3. In the General Properties area, 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 **Type** list, select the **MX** type.
5. In the Members area, for the **Load Balancing Method** setting, 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. 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. Add wide IPs as members of this load balancing pool.

The system evaluates the wide IPs (pool members) in the order in which they are listed. A wide IP can belong to more than one pool.

    a) In the Members area, for the **Member** setting, from the **Wide IP** list, select a wide IP or type a name that matches an existing wildcard wide IP.

    b) Click **Add**.

8. 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® DNS returns an SOA record that contains a TTL with a Return Code On Failure response. With this configuration, the local DNS servers can cache a negative response and 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 List 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 **Type** list, select one of these record types for the wide IP:

Option	Description
NAPTR	The Name Authority Pointer record, NAPTR, aids in the standardization of Uniform Resource Names (URNs). NAPTR records map between sets of URNs, URLs and plain domain names, and suggest to clients the protocols available for communication with the mapped resource.
A	The Address record, or A record, lists the IP address for a given host name.
SRV	The Service resource record, SRV, is a pointer with which an alias for a given service is redirected to another domain.
CNAME	The Canonical Name resource record, CNAME, specifies an alias or nickname for the official, or canonical, host name.
AAAA	The IPv6 Address record, or AAAA record, lists the 128-bit IPv6 address for a given host name.
MX	The Mail Exchange resource record, MX, defines the mail system(s) for a given domain.

6. From the **Return Code On Failure** list, select **Enabled**.

7. From the **RCODE** list, select one of these options:

Option	Description
NOERROR (No Error)	No error condition.

Option	Description
FORMERR (Query Format Error)	The name server was unable to interpret the query.
SERVFAIL (Server Failure)	The name server was unable to process this query due to a problem with the name server.
NXDOMAIN (Non Existent Domain)	The domain name referenced in the query does not exist.
NOTIMP (Not Implemented)	The name server does not support the requested kind of query.
REFUSED (Refuse To Answer)	The name server refuses to perform the specified operation for policy reasons.

8. In the **SOA Negative Caching TTL** field, type the number of seconds that the local DNS servers consider the Return Code On Failure to be valid.

9. In the Pools area, for the **Pool List** setting, 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**.

10. Click **Finished**.

Implementation result

You now have an implementation in which DNS returns a TTL in a Return Code On Failure for a web site represented by a wide IP in the BIG-IP DNS configuration.

Configuring a RCODE to Return a Response

Overview: Configuring an RCODE to return a response to the client when load balancing fails

You can use BIG-IP®DNS to configure a return code (RCODE) to return a response to the client when load balancing fails. Only when load balancing fails and the RCODE configuration is enabled, will an RCODE response be returned.

There are two types of load balancing failures where an RCODE response will be returned:

- When using all the Primary and Alternate methods for wide IP pools.
- When using a Return to DNS load balancing method.

Task summary

Perform these tasks to configure a return code (RCODE) to return a response to the client.
Creating a pool with an applicable pool type
Creating a wide IP that provides for returning a response with a RCODE

Creating a pool with an applicable pool type

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

Create a pool in order to configure the BIG-IP® system to load balance global traffic.

Creating a pool with pool type A or AAAA

Create an A or AAAA pool type in order to configure the BIG-IP® system to load balance global traffic.

1. On the Main tab, click **DNS** > **GSLB** > **Pools**.
   The Pool List screen opens.
2. Click **Create**.
3. In the General Properties area, 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 **Type** list, depending on the type of the system (IPv4 or IPv6), select either an **A** or **AAAA** pool type.
5. In the Configuration area, for the **Health Monitors** setting, in the **Available** list, select a monitor type, and move the monitor to the **Selected** list.

Tip: *Hold the Shift or Ctrl key to select more than one monitor at a time.*

6. In the Members area, for the **Load Balancing Method** setting, 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.*

7. 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.

8. In the Members area, 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**.

9. Click **Finished**.

Creating a pool with pool type NAPTR

Create an NAPTR pool type in order to configure the BIG-IP® system to load balance global traffic.

1. On the Main tab, click **DNS** > **GSLB** > **Pools**.
   The Pool List screen opens.

2. Click **Create**.

3. In the General Properties area, 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 **Type** list, select the **NAPTR** type.

5. In the Members area, for the **Load Balancing Method** setting, 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. 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. In the Members area, for the **Member List** setting, from the **Flags** list, select a flag.

8. Add wide IPs as members of this load balancing pool.

   The system evaluates the wide IPs (pool members) in the order in which they are listed. A wide IP can belong to more than one pool.

   a) From the **Wide IP** list, select a wide IP or type a name that matches an existing wildcard wide IP.

b) In the **Service** field, type the name of a service or protocol.

c) Click **Add**.

9. Click **Finished**.

Creating a pool with pool type SRV

Create a SRV pool type in order to configure the BIG-IP® system to load balance global traffic.

1. On the Main tab, click **DNS** > **GSLB** > **Pools**.
   The Pool List screen opens.

2. Click **Create**.

3. In the General Properties area, 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 **Type** list, select the **SRV** type.

5. In the Members area, for the **Load Balancing Method** setting, 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. 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. Add wide IPs as members of this load balancing pool.

   The system evaluates the wide IPs (pool members) in the order in which they are listed. A wide IP can belong to more than one pool.

   a) In the Members area, for the **Member** setting, from the **Wide IP** list, select a wide IP or type a name that matches an existing wildcard wide IP.

   b) In the **Port** field, type a port number.

   c) Click **Add**.

8. Click **Finished**.

Creating a pool with pool type CNAME

Create a CNAME pool type in order to configure the BIG-IP® system to load balance global traffic.

1. On the Main tab, click **DNS** > **GSLB** > **Pools**.
   The Pool List screen opens.

2. Click **Create**.

3. In the General Properties area, 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 **Type** list, select the **CNAME** type.

5. In the Members area, for the **Load Balancing Method** setting, 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. 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. Add wide IPs as members of this load balancing pool.

   The system evaluates the wide IPs (pool members) in the order in which they are listed. A wide IP can belong to more than one pool.

   a) In the Members area, for the **Member** setting, from the **Wide IP** list, select a wide IP or type a name that matches either an existing wildcard wide IP or wide IP alias.

   b) If necessary, to allow the member to point to a name that does not exist as a wide IP on DNS, select the **Static Target** check box.

   c) Click **Add**.

8. Click **Finished**.

Creating a pool with pool type MX

Create a MX pool type in order to configure the BIG-IP® system to load balance global traffic.

1. On the Main tab, click **DNS** > **GSLB** > **Pools**.
   The Pool List screen opens.

2. Click **Create**.

3. In the General Properties area, 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 **Type** list, select the **MX** type.

5. In the Members area, for the **Load Balancing Method** setting, 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. 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. Add wide IPs as members of this load balancing pool.

   The system evaluates the wide IPs (pool members) in the order in which they are listed. A wide IP can belong to more than one pool.

   a) In the Members area, for the **Member** setting, from the **Wide IP** list, select a wide IP or type a name that matches an existing wildcard wide IP.

    b) Click **Add**.

8. Click **Finished**.

Creating a wide IP that provides for returning a response with a RCODE

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

Create a wide IP that provides for configuring a return code (RCODE) to return a response to the client when load balancing fails.

1. On the Main tab, click **DNS** > **GSLB** > **Wide IPs**.
The Wide IP List screen opens.

2. Click **Create**.
The New Wide IP List 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 **Type** list, select one of these record types for the wide IP:

Option	Description
NAPTR	The Name Authority Pointer record, NAPTR, aids in the standardization of Uniform Resource Names (URNs). NAPTR records map between sets of URNs, URLs and plain domain names, and suggest to clients the protocols available for communication with the mapped resource.
A	The Address record, or A record, lists the IP address for a given host name.
SRV	The Service resource record, SRV, is a pointer with which an alias for a given service is redirected to another domain.
CNAME	The Canonical Name resource record, CNAME, specifies an alias or nickname for the official, or canonical, host name.
AAAA	The IPv6 Address record, or AAAA record, lists the 128-bit IPv6 address for a given host name.
MX	The Mail Exchange resource record, MX, defines the mail system(s) for a given domain.

6. From the **Return Code On Failure** list, select **Enabled**.

7. From the **RCODE** list, select one of these options:

Option	Description
NOERROR (No Error)	No error condition.
FORMERR (Query Format Error)	The name server was unable to interpret the query.
SERVFAIL (Server Failure)	The name server was unable to process this query due to a problem with the name server.
NXDOMAIN (Non Existent Domain)	The domain name referenced in the query does not exist.

Option	Description
NOTIMP (Not Implemented)	The name server does not support the requested kind of query.
REFUSED (Refuse To Answer)	The name server refuses to perform the specified operation for policy reasons.

8. Click **Finished**.

Implementation result

You now have an implementation in which DNS has a return code (RCODE) configured to return a response to the client when load balancing fails.

Configuring Device-Specific Probing and Statistics Collection

Overview: Configuring device-specific probing and statistics collection

BIG-IP® DNS 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 DNS 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 DNS 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 DNS 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 DNS 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:
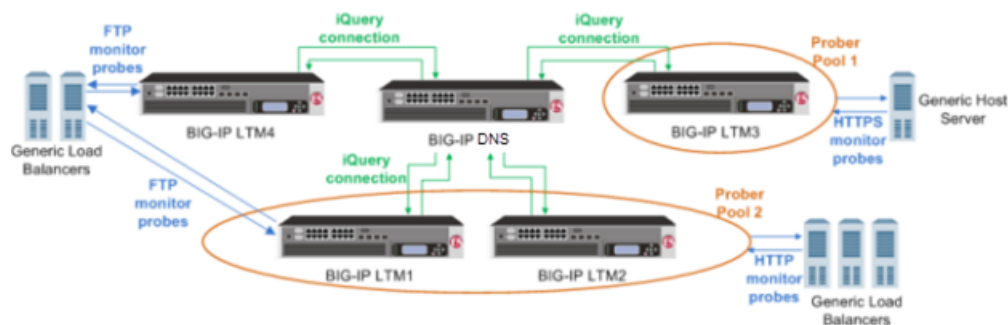
Figure 10: BIG-IP systems with prober pools

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 DNS 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 DNS 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 DNS system on which you are viewing status. Therefore, that BIG-IP DNS 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® DNS 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 DNS systems in a synchronization group. The statistics on one BIG-IP DNS include only the requests made from that BIG-IP DNS 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®DNS, 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® DNS, define a server that represents a physical server in your network. Repeat these steps for each server in your network, including the BIG-IP DNS 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 BIG-IP DNS 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 BIG-IP DNS system or for a BIG-IP DNS/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 BIG-IP DNS/LTM combo system when you want the BIG-IP DNS 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 BIG-IP DNS/LTM combo system when you want the BIG-IP DNS 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 DNS 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	BIG-IP DNS load balances monitor probes among the members of a Prober pool in a circular and sequential pattern.
Global Availability	BIG-IP DNS 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 Preference** 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 Preference** list, select one of the following.

Option	Description
Inside the Data Center	By default, a server selects the Prober pool from within the existing data center.
Outside the Data Center	A server selects the Prober pool from outside the existing data center.
Inherit from Data Center	A server inherits the Prober pool assigned to the data center in which the server resides.

4. From the **Prober Fallback** list, select one of the following.

Option	Description
Any available	By default, selects any available Prober pool.
Inside the Data Center	A server selects the Prober pool from within the existing data center.
Outside the Data Center	A server selects the Prober pool from outside the existing data center.
Inherit from Data Center	A server inherits the Prober pool assigned to the data center in which the server resides.
None	No Prober pool is used. Prober Fallback is disabled.

     5. 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® DNS 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.

Configuring How and When BIG-IP DNS Saves Configuration Changes

Overview: Configuring how and when BIG-IP DNS saves configuration changes

By default, BIG-IP® DNS automatically saves BIG-IP DNS configuration changes 15 seconds after the change is made in either the Configuration utility or tmsh. You can change how long BIG-IP DNS waits before it saves BIG-IP DNS configuration changes. In addition, you can disable automatic saves of BIG-IP DNS configuration changes, but then you must run a command in tmsh to save those changes. All changes to the BIG-IP DNS 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 BIG-IP DNS configuration changes.

Changing the automatic configuration save timeout
Enabling manual saves of configuration changes
Configuring how and when BIG-IP DNS saves configuration changes using tmsh

Changing the automatic configuration save timeout

Ensure that DNS is provisioned on the device.

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

   The values shown in the table are worth noting:

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

Enabling manual saves of configuration changes

Ensure that DNS is provisioned on the device.

You can disable automatic saves of BIG-IP DNS configuration changes when you want to have strict control over when BIG-IP DNS 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 BIG-IP DNS configuration changes.

   Important: *If you disable automatic saves of BIG-IP DNS 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 BIG-IP DNS saves configuration changes using tmsh

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

By default, the BIG-IP® system automatically saves BIG-IP DNS configuration changes made in the Configuration utility and `tmsh`. You can change how long the system waits to save BIG-IP DNS configuration changes. You can also configure the system for manual saves that require you to run a `tmsh` command to save BIG-IP DNS 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 BIG-IP DNS 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	BIG-IP DNS immediately saves changes to the configuration.
-1	BIG-IP DNS never saves changes to the configuration (manual save required).
86400	Maximum number of seconds following a BIG-IP DNS configuration change before the system saves the change.
15	Default number of seconds following a BIG-IP DNS configuration change before the system saves the change.

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

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

Load balancing Access Policy Manager

Overview: Load balancing BIG-IP APM with BIG-IP DNS

After you integrate BIG-IP® DNS into a network with BIG-IP Local Traffic Manager™ (LTM®), or vice versa, the BIG-IP systems can communicate with each other. If Access Policy Manager® (APM®) is also installed on one of the BIG-IP systems with LTM, APM calculates virtual server scores and provides them to BIG-IP DNS.

The calculation is based on the number of active access sessions. APM calculates two usage scores and assigns the higher of the two to the virtual server:

- One usage score is based on the BIG-IP system licensed maximum access concurrent sessions and the sum of the current active sessions on all the access profiles configured on the system.
- The other usage score is based on the maximum concurrent user sessions configured on the access profile attached to the virtual server and the current active sessions count on the access profile.

A value of 0 indicates no capacity and a value of 100 means full capacity available on the device.

Note: The calculations do not include connectivity session usage.

Use a BIG-IP DNS global load-balancing pool for BIG-IP DNS to load balance APM users based on the virtual server score. BIG-IP DNS uses virtual server score in the VS Score and Quality of Service load balancing methods for global load-balancing pools.

Task summary

These tasks must already be complete before you begin.

- BIG-IP DNS and APM must be installed and configured.
- Either BIG-IP DNS must be integrated with other BIG-IP systems on a network or BIG-IP LTM® must be integrated into a network with BIG-IP DNS.
- The health monitors defined for the BIG-IP DNS and LTM servers must include bigip; otherwise, APM does not calculate virtual server scores and send them to BIG-IP DNS.

Task list

Creating a load balancing pool
Creating a wide IP for BIG-IP DNS

Creating a load balancing pool

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

Create a pool of systems with Access Policy Manager® to which the system can load balance global traffic.

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

3. In the General Properties area, 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 **Type** list, depending on the type of the system (IPv4 or IPv6), select either an **A** or **AAAA** pool type.

5. In the Configuration area, for the **Health Monitors** setting, in the **Available** list, select a monitor type, and move the monitor to the **Selected** list.

   Tip: Hold the Shift or Ctrl key to select more than one monitor at a time.

   ---

6. In the Members area, for the **Load Balancing Method** settings, select a method that uses virtual server score:

   - VS Score - If you select this method, load balancing decisions are based on the virtual server score only.
   - Quality of Service - If you select this method, you must configure weights for up to nine measures of service, including **VS Score**. Virtual server score then factors into the load balancing decision at the weight you specify.

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**.

Creating a wide IP for BIG-IP DNS

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 an 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 List screen opens.

3. In the General Properties area, 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 **Type** list, select a record type for the wide IP.

5. In the Pools area, for the **Pool List** setting, 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**.

6. Click **Finished**.

Configuring Logging of Global Server Load Balancing Decisions

About logging global server load-balancing decisions

When BIG-IP® DNS 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 BIG-IP DNS 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® DNS 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 BIG-IP DNS 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)]
```

```
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)]
```

Monitoring Third-Party Servers with SNMP

Overview: SNMP monitoring of third-party servers

You can configure BIG-IP® DNS, formerly 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 DNS 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 DNS 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® DNS, 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 Preference** list, select one of the following.

Option	Description
Inside the Data Center	By default, a server selects the Prober pool from within the existing data center.
Outside the Data Center	A server selects the Prober pool from outside the existing data center.
Inherit from Data Center	A server inherits the Prober pool assigned to the data center in which the server resides.

8. From the **Prober Fallback** list, select one of the following.

Option	Description
Any available	By default, selects any available Prober pool.
Inside the Data Center	A server selects the Prober pool from within the existing data center.
Outside the Data Center	A server selects the Prober pool from outside the existing data center.
Inherit from Data Center	A server inherits the Prober pool assigned to the data center in which the server resides.
None	No Prober pool is used. Prober Fallback is disabled.

9. In the Health Monitors area, assign an SNMP monitor to the server by moving it from the **Available** list to the **Selected** list.

10. From the **Virtual Server Discovery** list, select **Disabled**.

11. 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**.

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

Implementation result

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

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

About BIG-IP DNS and DNS rate-limited license statistics

If you have a BIG-IP® DNS 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 DNS 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 BIG-IP DNS system handles based on the rate-limited license installed on the system.
Object Count	The sum of these objects configured on the BIG-IP DNS system: data centers, wide IPs, wide IP aliases, servers, pools, pool members, virtual servers, iRules®, and topology records.

Statistic type	Description
Rate Rejects	The number of DNS requests that the BIG-IP DNS system has rejected based on the rate limit of the license installed on the system.
	Tip: *The BIG-IP® DNS 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 BIG-IP DNS 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.*

How to Diagnose 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™ (BIG-IP DNS) 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® DNS configuration contains at least one BIG-IP server object with a self IP address.

To view information about the connections between BIG-IP DNS 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 DNS and the BIG-IP systems in your network, log in to that BIG-IP DNS 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®DNS.
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 Statistics	Description
iQuery State	Displays the state of the iQuery connection between the specified server and the BIG-IP DNS. Possible states are: • Not Connected • Connecting • Connected • Backlogged (indicates messages are queued and waiting to be sent)
iQuery Reconnects	Displays the number of times the BIG-IP DNS re-established an iQuery connection with the specified server.
Bytes In	Displays the amount of data in bytes received by the BIG-IP DNS over the iQuery connection from the specified server.
Bytes Out	Displays the amount of data in bytes sent from the BIG-IP DNS over the iQuery connection to the specified server.
Backlogs	Displays the number of times the iQuery connection between the BIG-IP DNS 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 BIG-IP DNS configuration was last modified. The timestamps should be the same for all devices in a BIG-IP DNS synchronization group.

Legal Notices

Legal notices

Publication Date

This document was published on June 21, 2018.

Publication Number

MAN-0592-01

Copyright

Trademarks

Patents

Export Regulation Notice

RF Interference Warning

FCC Compliance

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.

Index