# Table of Contents

Configuring DNS Express..........................................................................................................9
- What is DNS Express?...........................................................................................................9
- About configuring DNS Express..........................................................................................9
- Configuring DNS Express to answer DNS queries............................................................10
  - Example of loading a zone into DNS Express............................................................10
  - Example of DNS Express answering DNS queries....................................................10
  - About TSIG key authentication.....................................................................................11
  - About listeners...............................................................................................................11
- Task summary .....................................................................................................................12
  - Configuring BIND servers to allow zone transfers.....................................................12
  - Configuring local BIND to send NOTIFY messages to DNS Express.......................12
  - Adding TSIG keys.........................................................................................................13
  - Adding nameserver objects that represent DNS servers............................................13
  - Creating a DNS zone to answer DNS queries.............................................................14
  - Disabling TSIG verification for NOTIFY messages .....................................................14
  - Optional: Enabling DNS Express with a custom DNS profile ..................................15
  - Creating listeners to identify DNS queries.................................................................15
  - Viewing DNS zone statistics..........................................................................................16
- Configuring DNS Express to answer zone transfer requests.............................................16
  - Example of DNS Express answering zone transfer requests......................................17
- Task summary .....................................................................................................................17
  - Adding nameserver objects that represent DNS nameservers (clients)......................17
  - Configuring DNS Express to answer zone transfer requests from specified clients........18
  - Enabling DNS Express to respond to a zone transfer request.....................................18

Configuring Rapid Response to Mitigate DNS Flood Attacks...............................................19
- Overview: Configuring DNS Rapid Response.................................................................19
- About configuring DNS Rapid Response..........................................................................19
- Creating a DNS Rapid Response profile..........................................................................19
- Viewing DNS Rapid Response statistics........................................................................20

Configuring Protocol Validation and Response Cache.........................................................21
- Overview: Configuring Protocol Validation and Response Cache.....................................21
- Enabling a bitstream...........................................................................................................21
- Supported platforms for FPGA firmware selection.........................................................21
- Configuring Protocol Validation and Response Cache in a DNS profile.........................21
- Applying a DNS profile to a listener................................................................................22

Configuring a DNS Zone Proxy.............................................................................................23
- Overview: Configuring a DNS zone proxy.......................................................................23
  - Example of DNS zone proxy with client-side TSIG authentication...........................23
  - Example of DNS zone proxy with client-side and server-side TSIG authentication....24
- About TSIG key authentication.......................................................................................24
- About listeners...............................................................................................................25
- Task summary ...................................................................................................................25
  - Configuring BIND servers to allow zone transfers.....................................................25
Adding TSIG keys for DNS zone proxy ................................................................. 26
Adding DNS nameserver (client) objects ............................................................ 26
Enabling zone transfers .................................................................................... 27
Creating a DNS zone ......................................................................................... 27

Configuring BIG-IP to Load Balance Zone Transfer Requests to a Pool of DNS Servers .................................................................................................................................................................................................................................................. 29
Overview: Configuring BIG-IP to load balance zone transfer requests to a pool of DNS servers .................................................................................................................................................................................................................................................. 29
Example of load balancing zone transfer requests with client-side TSIG authentication to a pool .................................................................................................................................................................................................................................................. 29
Example of load balancing zone transfer requests with client-side and server-side TSIG authentication to a pool .................................................................................................................................................................................................................................................. 30
About TSIG key authentication ............................................................................ 30
About listeners .................................................................................................... 31
Task summary ........................................................................................................ 31
Configuring BIND servers to allow zone transfers ............................................ 31
Adding TSIG keys ............................................................................................... 32
Adding DNS nameserver (client) objects ............................................................ 32
Enabling zone transfers .................................................................................... 33
Creating a custom DNS monitor ......................................................................... 33
Creating a pool of local DNS servers for load balancing zone transfer requests .................................................................................................................................................................................................................................................. 34
Creating a DNS zone ......................................................................................... 34

Configuring DNSSEC .......................................................................................... 37
Introducing DNSSEC .......................................................................................... 37
About DNSSEC .................................................................................................... 37
About DNSSEC keys ........................................................................................... 37
About enhancing DNSSEC key security ................................................................ 37
About SEP records and DNSSEC ......................................................................... 38
About configuring DNSSEC ................................................................................ 39
About configuring basic DNSSEC ......................................................................... 39
Creating listeners to identify DNS traffic ........................................................... 40
Creating automatically managed DNSSEC zone-signing keys ......................... 40
Creating manually managed DNSSEC zone-signing keys .................................. 41
Creating automatically managed DNSSEC key-signing keys ........................... 42
Creating manually managed DNSSEC key-signing keys ................................... 43
Creating a DNSSEC zone .................................................................................. 44
Confirming that BIG-IP DNS is signing DNSSEC records ............................... 44
About configuring DNSSEC with an external HSM .......................................... 44
Creating listeners to identify DNS traffic ........................................................... 45
Creating automatically managed DNSSEC zone-signing keys for use with an external HSM .................................................................................................................................................................................................................................................. 45
Creating manually managed DNSSEC zone-signing keys for use with an external HSM .................................................................................................................................................................................................................................................. 46
Creating automatically managed DNSSEC key-signing keys for use with an external HSM .................................................................................................................................................................................................................................................. 47
Creating manually managed DNSSEC key-signing keys for use with an external HSM .................................................................................................................................................................................................................................................. 48
Creating a DNSSEC zone .................................................................................. 48
Confirming that BIG-IP DNS is signing DNSSEC records ............................... 49
Configuring DNSSEC with an internal HSM ..................................................... 49
Creating listeners to identify DNS traffic ........................................................... 50
Task summary .................................................................................................................. 89
  Adding forward zones to a DNS cache ..................................................................... 90
  Deleting forward zones from a DNS cache ............................................................ 90
  Changing the nameservers associated with a forward zone ..................................... 90
  Viewing statistics about DNS cache forward zones ................................................. 91
Overview: Forwarding specific DNS queries to a pool of DNS servers ..................... 91
  Creating a custom DNS monitor ............................................................................. 92
  Creating a pool of local DNS servers .................................................................... 92
  Creating a resolver DNS cache ............................................................................. 93
  Enabling resolving and caching ............................................................................ 93
  Creating listeners that alert BIG-IP DNS to DNS queries for a pool of DNS servers .. 93
  Configuring a forward zone with a listener that load balances DNS queries .......... 94
Overview: Customizing a DNS cache ...................................................................... 94
  Resolving DNS queries for default local zones from a DNS cache ....................... 95
  Using specific DNS servers as authoritative root nameservers ............................ 95
  Alerting the system to cache poisoning .................................................................. 95
  Configuring RRset Rotate to specify the order to return resource records ............ 96
Configuring DNS Response Policy Zones .................................................................. 97
  Overview: DNS response policy zones and the BIG-IP system .............................. 97
  About creating an RPZ using ZoneRunner .............................................................. 97
  Creating a custom RPZ using ZoneRunner .............................................................. 97
  Adding resource records to a custom RPZ ............................................................... 98
About configuring the BIG-IP system to use an RPZ as a DNS firewall .................... 99
  Optional: Adding a TSIG key for the server that hosts the RPZ .............................. 99
  Adding a nameserver object for the server that hosts the RPZ ............................... 99
  Creating an RPZ DNS Express zone ..................................................................... 100
  Creating a DNS cache .......................................................................................... 100
  Adding a local zone to represent a walled garden ............................................... 101
  Adding an RPZ to a DNS cache .......................................................................... 101
  Staging the RPZ on your network ........................................................................ 102
  Creating a custom DNS profile for DNS caching ............................................... 102
  Viewing DNS zone statistics .............................................................................. 103
  Viewing DNS cache statistics ............................................................................. 103
About configuring the BIG-IP system as an RPZ distribution point ......................... 103
  Configuring the BIG-IP system as a distribution point for an RPZ ....................... 104
  Enabling the BIG-IP system to respond to zone transfer requests ....................... 104
Configuring DNS64 ................................................................................................... 105
  Overview: Configuring DNS64 ............................................................................ 105
  Creating a custom DNS profile .......................................................................... 105
  Assigning a DNS profile to a DNS listener ........................................................... 106
Implementation result ............................................................................................... 107
Configuring IP Anycast (Route Health Injection) ....................................................... 109
  Overview: Configuring IP Anycast (Route Health Injection) ............................... 109
  Enabling the ZebOS dynamic routing protocol ..................................................... 109
  Creating a custom DNS profile .......................................................................... 109
  Configuring a listener for route advertisement .................................................... 110
  Verifying advertisement of the route .................................................................. 111
Implementation result ............................................................................................... 111
# Configuring Remote High-Speed DNS Logging

- Overview: Configuring remote high-speed DNS logging .................................................. 113
- About the configuration objects of remote high-speed DNS logging ...................................... 114
- Creating a pool of remote logging servers ........................................................................ 115
- Creating a remote high-speed log destination .................................................................... 115
- Creating a formatted remote high-speed log destination .................................................... 116
- Creating a publisher ........................................................................................................ 116
- Creating a custom DNS logging profile for logging DNS queries ........................................ 116
- Creating a custom DNS logging profile for logging DNS responses ................................... 117
- Creating a custom DNS logging profile for logging DNS queries and responses ................. 117
- Creating a custom DNS profile to enable DNS logging ..................................................... 118
- Disabling DNS logging ..................................................................................................... 119
- Implementation result........................................................................................................ 119

# Setting Up and Viewing DNS Statistics

- Overview: Setting up and viewing DNS statistics ............................................................ 121
- Creating a DNS profile for AVR statistics collection ........................................................ 121
- Configuring a BIG-IP DNS listener for DNS AVR statistics collection ............................. 122
- Viewing DNS AVR statistics .......................................................................................... 122
- Viewing DNS AVR statistics in tmsh .............................................................................. 123
- Viewing DNS global statistics ....................................................................................... 123
- Viewing DNS statistics for a specific virtual server .......................................................... 123
- Implementation result...................................................................................................... 124

# Using ZoneRunner to Configure DNS Zones

- Overview: ZoneRunner ...................................................................................................... 125
- About ZoneRunner ........................................................................................................... 125
- About named.conf ............................................................................................................ 125
- Creating a master DNS zone .......................................................................................... 125
- Creating a hint zone ........................................................................................................ 126
- Configuring BIG-IP DNS to allow zone file transfers ...................................................... 126
- About DNS views .......................................................................................................... 128
- Types of DNS zone files ............................................................................................... 129
- Types of DNS resource records .................................................................................... 129

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

- Overview: Troubleshooting a BIG-IP System with a Rate-Limited License ......................... 131
- About BIG-IP DNS and DNS rate-limited license statistics .............................................. 131
- Viewing rate-limited license statistics ............................................................................ 131

# Legal Notices

- Legal notices .................................................................................................................... 133
Configuring DNS Express

What is DNS Express?

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

About configuring DNS Express

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

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

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

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

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

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

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

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

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

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

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

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

Example of loading a zone into DNS Express

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

Figure 1: DNS zone transfer to DNS Express

1. Creation of siterequest.com DNS zone with a DNS Express server on the BIG-IP system initiates an unsolicited zone transfer request for siterequest.com (server TSIG key optional).
2. Zone transfer of siterequest.com to DNS Express (server TSIG key optional).

Example of DNS Express answering DNS queries

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

Figure 2: DNS Express answering queries for a DNS zone

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

About TSIG key authentication

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

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

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

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

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

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

About listeners

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

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

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

Configuring BIND servers to allow zone transfers

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

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

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

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

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

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

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

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

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

Configuring local BIND to send NOTIFY messages to DNS Express

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

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

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

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

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

Add TSIG keys to the BIG-IP system configuration, in these cases:
- When you want to validate zone transfer communications between DNS Express and a DNS server.
- When you want to validate zone transfer communications between DNS Express and a DNS nameserver (client).

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

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

Adding nameserver objects that represent DNS servers

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

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

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

The BIG-IP system uses this TSIG key to sign DNS zone transfer requests sent to the DNS server that hosts this zone, and then to verify a zone transfer returned from the DNS server.
Create a DNS zone and add a DNS Express server object to the zone.

Creating a DNS zone to answer DNS queries

Before you create a DNS zone, you must:

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

Note: Zone names are not case-sensitive.

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

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

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

5. From the Notify Action list, select one of the options to specify the action the DNS Express engine takes after receiving a NOTIFY message for this zone.

<table>
<thead>
<tr>
<th>Action</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Consume</td>
<td>NOTIFY messages go to the DNS Express engine. This is the default value.</td>
</tr>
<tr>
<td>Bypass</td>
<td>NOTIFY messages do not go to the DNS Express engine, but instead go to a DNS server (subject to DNS profile unhandled-query-action).</td>
</tr>
<tr>
<td>Repeat</td>
<td>NOTIFY messages go to both the DNS Express engine and a DNS server.</td>
</tr>
</tbody>
</table>

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

6. For the Allow NOTIFY From setting, in the Address field, type an IP address from which the BIG-IP system will accept NOTIFY messages for the DNS Express zone.

Note: The IP address of the authoritative primary DNS Server selected in step 4 is allowed by default, and does not need to be entered.

7. Click Finished.

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

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

Optional: Enabling DNS Express with a custom DNS profile

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

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

1. On the Main tab, click DNS > Delivery > Profiles > DNS or Local Traffic > Profiles > Services > DNS.
   The DNS profile list screen opens.
2. Click Create.
   The New DNS Profile screen opens.
3. In the General Properties area, name the profile dns_express.
4. In the General Properties area, from the Parent Profile list, accept the default dns profile.
5. Select the Custom check box.
6. In the DNS Features area, from the GSLB list, select Disabled.
7. In the DNS Features area, from the DNS Express list, retain the default value Enabled.
8. In the DNS Features area, from the Unhandled Query Actions list, select how you want the BIG-IP system to handle a query that is not for a wide IP or DNS Express zone.

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

9. In the DNS Features area, from the Use BIND Server on BIG-IP list, select Disabled.
10. Click Finished.

Assign the profile to virtual servers or listeners.

Creating listeners to identify DNS queries

Create listeners to identify the DNS queries that DNS Express handles. When DNS Express® is only answering DNS queries, only two listeners are required: one with an IPv4 address that handles UDP traffic and one with an IPv6 address that handles UDP traffic.
However, the best practice is to create four listeners, which allows DNS Express to handle zone transfers, should you decide to use this feature. DNS zone transfers use TCP port 53. With this configuration, you create one listener with an IPv4 address that handles UDP traffic, and one with the same IPv4 address that handles TCP traffic. You also create one listener with an IPv6 address that handles UDP traffic, and one with the same IPv6 address that handles TCP traffic.

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

**Note:** These steps apply only to BIG-IP® DNS-provisioned systems.

1. On the Main tab, click DNS > Delivery > Listeners.
   The Listeners List screen opens.
2. Click Create.
   The Listeners properties screen opens.
3. In the Name field, type a unique name for the listener.
4. For the Destination setting, in the Address field, type an IPv4 address on which the BIG-IP system listens for DNS queries.
5. From the Listener list, select Advanced.
6. (Optional) If you are using SNATs on your network, from the Source Address Translation list, select SNAT.
7. Optional: If you are using NATs on your network, for the Address Translation setting, select the Enabled check box.
8. Optional: If you are using port translation on your network, for the Port Translation setting, select the Enabled check box.
9. In the Service area, from the Protocol list, select UDP.
10. In the Service area, from the DNS Profile list, select either dns or a custom DNS profile configured for DNS Express.
11. Click Finished.

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

**Viewing DNS zone statistics**

You can view information about DNS zones.

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

**Configuring DNS Express to answer zone transfer requests**

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

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

![Diagram of DNS Express answering zone transfer requests]

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

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

Task summary

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

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

Adding nameserver objects that represent DNS nameservers (clients)

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

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

1. On the Main tab, click DNS > Delivery > Nameservers.
   The Nameservers List screen opens.
2. Click Create.
   The New Nameserver screen opens.
3. In the Name field, type a name for the DNS nameserver (client).
4. In the Address field, type the IP address on which the DNS nameserver (client) listens for DNS messages.
5. Optional: From the TSIG Key list, select the TSIG key you want the BIG-IP system to use to validate zone transfer traffic.
6. Click Finished.
7. Add nameserver objects to represent other DNS nameservers (clients).

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

Configuring DNS Express to answer zone transfer requests from specified clients

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

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

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

Enabling DNS Express to respond to a zone transfer request

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

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

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

Overview: Configuring DNS Rapid Response

When the BIG-IP® system is processing authoritative DNS responses for domains on your network using DNS Express, you can configure DNS Rapid Response to protect your network from DNS flood attacks on those domains.

DNS Rapid Response uses the maximum system resources available to mitigate a DNS attack. Statistics are available that show the number of DNS queries handled, the number of DNS responses generated, and the number of dropped DNS queries. However, when this feature is enabled, the system does not log DNS requests and responses.

If you enable the Rapid Response Mode for a Rapid Response profile, only global server load balancing (GSLB) and DNS Express will function.

About configuring DNS Rapid Response

When DNS Rapid Response is enabled on a DNS profile attached to a BIG-IP® Local Traffic Manager™ (LTM™) virtual server or DNS listener, system validation can cause a configuration load failure. When this occurs, an administrator can change the options on the DNS profile and load the configuration again. When the configuration loads, system validation may display entries in the logs in /var/log/ltm.

Before creating a DNS Rapid Response profile, you should be aware of the configurations in the following table that result in system validation errors and warnings, once DNS Rapid Response is enabled.

<table>
<thead>
<tr>
<th>Configuration</th>
<th>Validation Result</th>
</tr>
</thead>
<tbody>
<tr>
<td>Protocol other than UDP associated with BIG-IP DNS listener or LTM virtual server</td>
<td>Error. DNS profile fails to load.</td>
</tr>
<tr>
<td><strong>Auto Last Hop</strong> disabled on BIG-IP DNS listener or LTM virtual server</td>
<td>Error. DNS profile fails to load.</td>
</tr>
<tr>
<td>LTM iRule associated with an LTM virtual server</td>
<td>Warning. Matching DNS queries do not cause the iRules to run.</td>
</tr>
<tr>
<td>LTM pool associated with LTM virtual server</td>
<td>Warning. Matching DNS queries are not load balanced to the pool.</td>
</tr>
<tr>
<td>Additional profiles associated with BIG-IP DNS listener or LTM virtual server</td>
<td>Warning. Matching DNS queries do not activate features enabled on other profiles.</td>
</tr>
</tbody>
</table>

Creating a DNS Rapid Response profile

To protect your network on a BIG-IP® system from a DNS flood attack, configure a custom DNS Rapid Response profile.

*Note:* DNS Rapid Response works only for traffic over the UDP protocol.
1. On the Main tab, click **DNS > Delivery > Profiles > DNS**. The DNS list screen opens.

2. Click **Create**. The New DNS Profile screen opens.

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

4. In the General Properties area, from the **Parent Profile** list, accept the default **dns** profile.

5. Select the **Custom** check box.

6. In the Denial of Service Protection area, from the **Rapid Response Mode** list, select **Enabled**.

   **Note:** Enable this setting after a DNS flood attack occurs. When you enable, all other DNS features are disabled, except for DNS Express and global server load balancing (GSLB), unless the **Rapid Response Last Action** is set to **Allow**.

7. In the Denial of Service Protection area, from the **Rapid Response Last Action** list, select an option to protect your network:

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Allow</td>
<td>BIG-IP system sends non-matching DNS queries along the regular packet processing path</td>
</tr>
<tr>
<td>Drop</td>
<td>BIG-IP system drops the message without sending a response to the client. This is the default value.</td>
</tr>
<tr>
<td>No Error</td>
<td>BIG-IP system returns NOERROR response to the client.</td>
</tr>
<tr>
<td>NX Domain</td>
<td>BIG-IP system returns non-existent name response to the client.</td>
</tr>
<tr>
<td>Refuse</td>
<td>BIG-IP system returns REFUSED response to the client.</td>
</tr>
<tr>
<td>Truncate</td>
<td>BIG-IP system truncates the response to the client.</td>
</tr>
</tbody>
</table>

8. Click **Finished**.

**Viewing DNS Rapid Response statistics**

Ensure that you configure the BIG-IP® system for DNS Rapid Response.

View statistics about DNS Rapid Response traffic to debug network traffic problems.

1. On the Main tab, click **DNS > Delivery > Listeners > Statistics**. The Listeners screen opens.

2. In the Details column of a Listener, click **View**.

3. In the Profiles area, for the **Select Profile** settings list, select a DNS profile.

4. In the Rapid Response area, view the list of statistics.
Configuring Protocol Validation and Response Cache

Overview: Configuring Protocol Validation and Response Cache

You can configure Protocol Validation so that responses, both authoritative and non-authoritative, are cached to hardware in order to mitigate against random source flood attacks. By configuring DNS Response Cache to offload/accelerate commonly requested entries in hardware, entries can still be responded to when the software is overwhelmed.

If you have a DNS Services rate-limited license, Response Cache is automatically disabled.

Task summary

* Enabling a bitstream
* Configuring Protocol Validation and Response Cache in a DNS profile
* Applying a DNS profile to a listener

Enabling a bitstream

Ensure you are using a VIPRION® platform that supports FPGA firmware.

Enable the intelligent bitstream as part of the process to configure Protocol Validation and Response Cache.

2. For the FPGA Firmware Selection setting, select the i7-intelligent-fpga check box.

*Note: This setting is hidden if the appropriate hardware is not present.*

3. Click Submit.

Supported platforms for FPGA firmware selection

<table>
<thead>
<tr>
<th>Platform family</th>
<th>Platform model</th>
</tr>
</thead>
<tbody>
<tr>
<td>VIPRION®</td>
<td>B2250 blade</td>
</tr>
<tr>
<td>VIPRION</td>
<td>C2200 chassis</td>
</tr>
<tr>
<td>VIPRION</td>
<td>C2400 chassis</td>
</tr>
</tbody>
</table>

*Note: Hardware DNS features are only available on platforms that support Altera FPGA, including Vic2 and later platforms.*

Configuring Protocol Validation and Response Cache in a DNS profile

Ensure that the BIG-IP® system has a DNS Services license.

Configure Protocol Validation for dropping malformed packets and Response Cache to offload/accelerate commonly asked entries in hardware.
1. On the Main tab, click DNS > Delivery > Profiles > DNS. 
   The DNS list screen opens.
2. In the name column, click the system-supplied dns profile. 
   The DNS properties list screen opens.
3. In the Hardware Acceleration area, from the Protocol Validation list, select Enabled.
4. From the Response Cache list, select Enabled.
5. Click Update.

**Applying a DNS profile to a listener**

Apply a DNS profile as part of the process to configure Protocol Validation and Response Cache.

1. On the Main tab, click DNS > Delivery > Listeners. 
   The Listeners List screen opens.
2. In the Name column, click the name of a listener you want to modify.
3. In the Service area, for the DNS Profile setting, select the dns profile.

---

*Note: When the listener is defined from the BIG-IP® LTM® Virtual Server page, select the udp_gtm_dns profile.*

4. Click Update.
Configuring a DNS Zone Proxy

Overview: Configuring a DNS zone proxy

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

Example of DNS zone proxy with client-side TSIG authentication

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

![Figure 4: BIG-IP system acting as DNS zone proxy with client-side TSIG authentication](image)

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

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

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

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

About TSIG key authentication

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

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

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

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

- **Client sends TSIG-signed zone transfer request**

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

- **Client sends unsigned zone transfer request**

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

**About listeners**

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

**Task summary**

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

- Configuring BIND servers to allow zone transfers
- Adding TSIG keys for DNS zone proxy
- Adding DNS nameserver (client) objects
- Enabling zone transfers
- Creating a DNS zone

**Configuring BIND servers to allow zone transfers**

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

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

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

Here is an example allow-transfer statement that you can modify to meet your needs:

```bash
allow-transfer { localhost; <self IP address on BIG-IP from which zone transfer request is sent to the DNS server>; }
```
Adding TSIG keys for DNS zone proxy

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

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

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

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

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

Adding DNS nameserver (client) objects

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

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

1. On the Main tab, click **DNS > Delivery > Nameservers.**
   The Nameservers List screen opens.
2. Click **Create.**
   The New Nameserver screen opens.
3. In the **Name** field, type a name for the DNS nameserver (client).
4. In the **Address** field, type the IP address on which the DNS nameserver (client) listens for DNS messages.
5. Optional: From the **TSIG Key** list, select the TSIG key that matches the TSIG key on the DNS nameserver (client).
   The BIG-IP system uses this TSIG key to authenticate zone transfer communications as coming from this client and to sign communications sent to this client.
6. Click **Finished.**
7. Add nameserver objects to represent other DNS nameservers (clients).

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

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

1. On the Main tab, click DNS > Delivery > Profiles > DNS or Local Traffic > Profiles > Services > DNS.
   The DNS profile list screen opens.
2. Click Create.
   The New DNS Profile screen opens.
3. In the General Properties area, name the profile dns_zxfr.
4. Select the Custom check box.
5. In the DNS Features area, from the DNS Express list, select Disabled.
6. In the DNS Traffic area, from the Zone Transfer list, select Enabled.
7. In the DNS Features area, from the Unhandled Query Actions list, select Allow.
   The BIG-IP system forwards zone transfer requests to a DNS server or a member of a pool of DNS servers.
8. In the DNS Features area, from the Use BIND Server on BIG-IP list, select Disabled.
9. Click Finished.

Assign the profile to listeners.

Creating a DNS zone

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

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

**Note:** Zone names are case insensitive.

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

1. On the Main tab, click DNS > Zones.
   The Zone List screen opens.
2. Click Create.
   The New Zone screen opens.
3. In the Name field, type the name of the DNS zone.
   The name must begin and end with a letter and contain only letters, numbers, and the period and hyphen (-) characters.
4. In the Zone Transfer Clients area, move the nameservers that can initiate zone transfers from the Available list to the Active list.
5. Optional: From the Server Key list, select the TSIG key that matches the TSIG key on the DNS server.
   The BIG-IP system uses this TSIG key to sign DNS zone transfer requests, before forwarding the requests to the DNS server that hosts this zone, and then to verify a zone transfer returned from the DNS server.
6. Click Finished.
Overview: Configuring BIG-IP to load balance zone transfer requests to a pool of DNS servers

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

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

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

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

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

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

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

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

About TSIG key authentication

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

TSIG key configured on authoritative DNS server

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

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

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

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

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

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

- Configuring BIND servers to allow zone transfers
- Adding TSIG keys
- Adding DNS nameserver (client) objects
- Enabling zone transfers
- Creating a custom DNS monitor
- Creating a pool of local DNS servers for load balancing zone transfer requests
- Creating a DNS zone

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

Typically, BIND servers allow zone transfers to any DNS nameserver requesting a zone transfer. That is, named.conf on a typical BIND server does not contain an allow-transfer statement. Therefore, adding an allow-transfer statement to a BIND server actually restricts zone transfers to a specified list of DNS nameservers.
When you want the BIG-IP® system to act as a proxy for a DNS zone configured on a BIND server, you must add an `allow-transfer` statement to `named.conf` on the BIND server that hosts the zone.

Here is an example allow-transfer statement that you can modify to meet your needs:

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

### Adding TSIG keys

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

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

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

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

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

### Adding DNS nameserver (client) objects

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

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

1. On the Main tab, click **DNS > Delivery > Nameservers.**
   The Nameservers List screen opens.
2. Click **Create.**
   The New Nameserver screen opens.
3. In the **Name** field, type a name for the DNS nameserver (client).
4. In the **Address** field, type the IP address on which the DNS nameserver (client) listens for DNS messages.
5. Optional: From the **TSIG Key** list, select the TSIG key that matches the TSIG key on the DNS nameserver (client).
   The BIG-IP system uses this TSIG key to authenticate zone transfer communications as coming from this client and to sign communications sent to this client.
6. Click **Finished**.
7. Add nameserver objects to represent other DNS nameservers (clients).
   Add the DNS nameservers (clients) objects to the **Zone Transfer Client** list of the DNS zone on the BIG-IP system.

### Enabling zone transfers

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

1. On the Main tab, click **DNS > Delivery > Profiles > DNS** or **Local Traffic > Profiles > Services > DNS**.
   The DNS profile list screen opens.
2. Click **Create**.
   The New DNS Profile screen opens.
3. In the General Properties area, name the profile **dns_zxfr**.
4. Select the **Custom** check box.
5. In the DNS Features area, from the **DNS Express** list, select **Disabled**.
6. In the DNS Traffic area, from the **Zone Transfer** list, select **Enabled**.
7. In the DNS Features area, from the **Unhandled Query Actions** list, select **Allow**.
   The BIG-IP system forwards zone transfer requests to a DNS server or a member of a pool of DNS servers.
8. In the DNS Features area, from the **Use BIND Server on BIG-IP** list, select **Disabled**.
9. Click **Finished**.
   Assign the profile to listeners.

### Creating a custom DNS monitor

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

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

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

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

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

1. On the Main tab, click 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. Add each DNS server that you want to include in the pool using the New Members setting:
   a) In the Address field, type the IP address of the DNS server.
   b) Type 53 in the Service Port field.
   c) (Optional) Type a priority number in the Priority field.
   d) Click Add.

6. Click Finished.

Creating a DNS zone

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

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

Note: Zone names are case insensitive.

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

1. On the Main tab, click DNS > Zones.

   The Zone List screen opens.

2. Click Create.

   The New Zone screen opens.

3. In the Name field, type the name of the DNS zone.

   The name must begin and end with a letter and contain only letters, numbers, and the period and hyphen (-) characters.

4. In the Zone Transfer Clients area, move the nameservers that can initiate zone transfers from the Available list to the Active list.
5. Optional: From the **Server Key** list, select the TSIG key that matches the TSIG key on the members of the pool of DNS servers that host this zone.

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

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

About DNSSEC keys

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

About enhancing DNSSEC key security

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

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

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

About SEP records and DNSSEC

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

Obtaining a trust or DLV anchor

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

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

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

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

Figure 9: Traffic flow when BIG-IP DNS is the DNSSEC authoritative nameserver

About configuring basic DNSSEC

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

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

Task summary

Perform these tasks to configure DNSSEC on BIG-IP DNS.

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

Creating automatically managed DNSSEC zone-signing keys

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

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

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

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

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

1. On the Main tab, click **DNS > Delivery > Keys > DNSSEC Key List**.
   The DNSSEC Key List screen opens.
2. Click **Create**.
   The New DNSSEC Key screen opens.
3. In the **Name** field, type a name for the key.
   Zone names are limited to 63 characters.
4. From the **Type** list, select **Zone Signing Key**.
5. From the **State** list, select **Enabled**.
6. From the **Hardware Security Module** list, select **None**.
7. From the **Algorithm** list, select the digest algorithm the system uses to generate the key signature. Your options are **RSA/SHA1**, **RSA/SHA256**, and **RSA/SHA512**.
8. From the **Key Management** list, select **Automatic**.
   The Key Settings area displays fields for key configuration.
9. In the **Bit Width** field, type **1024**.
10. In the **TTL** field, accept the default value of **86400** (the number of seconds in one day.)
    This value specifies how long a client resolver can cache the key. This value must be less than the difference between the values of the rollover and expiration periods of the key; otherwise, a client can make a query and the system can send a valid key that the client cannot recognize.
11. For the Rollover Period setting, in the **Days** field, type **21**.
12. For the Expiration Period setting, in the **Days** field, type **30**.
    Zero seconds indicates not set, and thus the key does not expire.
13. For the Signature Validity Period setting, accept the default value of seven days.
    This value must be greater than the value of the signature publication period.
    Zero seconds indicates not set, and thus the server verifying the signature never succeeds, because the signature is always expired.
14. For the Signature Publication Period setting, accept the default value of four days and 16 hours.
    This value must be less than the value of the signature validity period.
    Zero seconds indicates not set, and thus the signature is not cached.
15. Click **Finished**.
16. To create a standby key for emergency rollover purposes, repeat these steps using a similar name, and select **Disabled** from the **State** list.

**Creating manually managed DNSSEC zone-signing keys**

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

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

---

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

---

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

1. On the Main tab, click **DNS > Delivery > Keys > DNSSEC Key List**.
   The DNSSEC Key List screen opens.
2. Click **Create**.
   The New DNSSEC Key screen opens.
3. In the **Name** field, type a name for the key.
   Zone names are limited to 63 characters.
4. From the **Type** list, select **Zone Signing Key**.
5. From the **State** list, select **Enabled**.
6. From the **Hardware Security Module** list, select **None**.
7. From the Algorithm list, select the digest algorithm the system uses to generate the key signature. Your options are RSA/SHA1, RSA/SHA256, and RSA/SHA512.

8. From the Key Management list, select Manual.
   The Key Settings area displays Certificate and Private Key lists.

9. In the Key Settings area, select a certificate/key pair:
   a) From the Certificate list, select a certificate.
   b) From the Private Key list, select the key that matches the certificate you selected.

10. Click Finished.

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

Creating automatically managed DNSSEC key-signing keys

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

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

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

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

Create key-signing keys for BIG-IP DNS to use in the DNSSEC authentication process.

1. On the Main tab, click DNS > Delivery > Keys > DNSSEC Key List.
   The DNSSEC Key List screen opens.

2. Click Create.
   The New DNSSEC Key screen opens.

3. In the Name field, type a name for the key.
   Zone names are limited to 63 characters.

4. From the Type list, select Key Signing Key.

5. From the State list, select Enabled.

6. From the Hardware Security Module list, select None.

7. From the Algorithm list, select the digest algorithm the system uses to generate the key signature.
   Your options are RSA/SHA1, RSA/SHA256, and RSA/SHA512.

8. From the Key Management list, select Automatic.
   The Key Settings area displays fields for key configuration.

9. In the Bit Width field, type 2048.

10. In the TTL field, accept the default value of 86400 (the number of seconds in one day.)

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

11. For the Rollover Period setting, in the Days field, type 340.
12. For the Expiration Period setting, in the Days field, type 365.
Zero seconds indicates not set, and thus the key does not expire.

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

13. For the Signature Validity Period setting, accept the default value of seven days.
This value must be greater than the value of the signature publication period.
Zero seconds indicates not set, and thus the server verifying the signature never succeeds, because the signature is always expired.

14. For the Signature Publication Period setting, accept the default value of four days and 16 hours.
This value must be less than the value of the signature validity period.
Zero seconds indicates not set, and thus the signature is not cached.

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

---

**Creating manually managed DNSSEC key-signing keys**

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

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

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

Create key-signing keys for BIG-IP DNS to use in the DNSSEC authentication process.

1. On the Main tab, click **DNS > Delivery > Keys > DNSSEC Key List**.
The DNSSEC Key List screen opens.

2. Click **Create**.
The New DNSSEC Key screen opens.

3. In the **Name** field, type a name for the key.
Zone names are limited to 63 characters.

4. From the **Type** list, select **Key Signing Key**.

5. From the **State** list, select **Enabled**.

6. From the **Hardware Security Module** list, select **None**.

7. From the **Algorithm** list, select the digest algorithm the system uses to generate the key signature.
Your options are RSA/SHA1, RSA/SHA256, and RSA/SHA512.

8. From the **Key Management** list, select **Manual**.
The Key Settings area displays **Certificate** and **Private Key** lists.

9. In the Key Settings area, select a certificate/key pair:
   a) From the **Certificate** list, select a certificate.
   b) From the **Private Key** list, select the key that matches the certificate you selected.

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

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

**Important:** The DNSSEC feature is available only when the BIG-IP system is licensed for BIG-IP DNS.

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

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

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

Confirming that BIG-IP DNS is signing DNSSEC records

After you create DNSSEC zones and zone-signing keys, you can confirm that BIG-IP® DNS is signing the DNSSEC records.

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

About configuring DNSSEC with an external HSM

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

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

**Task summary**
Perform these tasks to configure DNSSEC on BIG-IP DNS.
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.

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

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

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

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

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

Create zone-signing keys for BIG-IP DNS to use in the DNSSEC authentication process.
1. On the Main tab, click **DNS > Delivery > Keys > DNSSEC Key List.**
   The DNSSEC Key List screen opens.
2. Click **Create.**
   The New DNSSEC Key screen opens.
3. In the **Name** field, type a name for the key.
   Zone names are limited to 63 characters.
4. From the **Type** list, select **Zone Signing Key.**
5. From the **State** list, select **Enabled.**
6. From the **Hardware Security Module** list, select **External,** if you use a network HSM.
7. From the **Algorithm** list, select the digest algorithm the system uses to generate the key signature.
   Your options are **RSA/SHA1,** **RSA/SHA256,** and **RSA/SHA512.**
8. From the **Key Management** list, select **Automatic.**
   The Key Settings area displays fields for key configuration.
9. In the **Bit Width** field, type **1024.**
10. In the **TTL** field, accept the default value of **86400** (the number of seconds in one day.)
    This value specifies how long a client resolver can cache the key. This value must be less than the
difference between the values of the rollover and expiration periods of the key; otherwise, a client can
make a query and the system can send a valid key that the client cannot recognize.
11. For the Rollover Period setting, in the **Days** field, type **21.**
12. For the Expiration Period setting, in the **Days** field, type **30.**
    Zero seconds indicates not set, and thus the key does not expire.
13. For the Signature Validity Period setting, accept the default value of seven days.
    This value must be greater than the value of the signature publication period.
    Zero seconds indicates not set, and thus the server verifying the signature never succeeds, because the
signature is always expired.
14. For the Signature Publication Period setting, accept the default value of four days and 16 hours.
    This value must be less than the value of the signature validity period.
    Zero seconds indicates not set, and thus the signature is not cached.
15. Click **Finished.**
16. To create a standby key for emergency rollover purposes, repeat these steps using a similar name, and
    select **Disabled** from the **State** list.

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

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

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

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

Create zone-signing keys for BIG-IP DNS to use in the DNSSEC authentication process.
1. On the Main tab, click **DNS > Delivery > Keys > DNSSEC Key List.**
   The DNSSEC Key List screen opens.
2. Click **Create.**
   The New DNSSEC Key screen opens.
3. In the **Name** field, type a name for the key.
Zone names are limited to 63 characters.

4. From the **Type** list, select **Zone Signing Key**.

5. From the **State** list, select **Enabled**.

6. From the **Hardware Security Module** list, select **External**, if you use a network HSM.

7. From the **Algorithm** list, select the digest algorithm the system uses to generate the key signature.
Your options are **RSA/SHA1**, **RSA/SHA256**, and **RSA/SHA512**.

8. From the **Key Management** list, select **Manual**.
The Key Settings area displays **Certificate** and **Private Key** lists.

9. In the Key Settings area, select a certificate/key pair:
   a) From the **Certificate** list, select a certificate.
   b) From the **Private Key** list, select the key that matches the certificate you selected.

10. Click **Finished**.

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

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

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

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

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

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

Create key-signing keys for BIG-IP DNS to use in the DNSSEC authentication process.

1. On the Main tab, click **DNS > Delivery > Keys > DNSSEC Key List**.
The DNSSEC Key List screen opens.

2. Click **Create**.
The New DNSSEC Key screen opens.

3. In the **Name** field, type a name for the key.
Zone names are limited to 63 characters.

4. From the **Type** list, select **Key Signing Key**.

5. From the **State** list, select **Enabled**.

6. From the **Hardware Security Module** list, select **External**, if you use a network HSM.

7. From the **Algorithm** list, select the digest algorithm the system uses to generate the key signature.
Your options are **RSA/SHA1**, **RSA/SHA256**, and **RSA/SHA512**.

8. From the **Key Management** list, select **Automatic**.
The Key Settings area displays fields for key configuration.
9. In the **Bit Width** field, type 2048.

10. In the **TTL** field, accept the default value of 86400 (the number of seconds in one day.)
    This value specifies how long a client resolver can cache the key. This value must be less than the difference between the values of the rollover and expiration periods of the key; otherwise, a client can make a query and the system can send a valid key that the client cannot recognize.

11. For the Rollover Period setting, in the **Days** field, type 340.

12. For the Expiration Period setting, in the **Days** field, type 365.
    Zero seconds indicates not set, and thus the key does not expire.

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

13. For the Signature Validity Period setting, accept the default value of seven days.
    This value must be greater than the value of the signature publication period.
    Zero seconds indicates not set, and thus the server verifying the signature never succeeds, because the signature is always expired.

14. For the Signature Publication Period setting, accept the default value of four days and 16 hours.
    This value must be less than the value of the signature validity period.
    Zero seconds indicates not set, and thus the signature is not cached.

15. Click **Finished**.

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

---

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

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

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

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

Create key-signing keys for BIG-IP DNS to use in the DNSSEC authentication process.

1. On the Main tab, click **DNS > Delivery > Keys > DNSSEC Key List**.
   The DNSSEC Key List screen opens.

2. Click **Create**.
   The New DNSSEC Key screen opens.

3. In the **Name** field, type a name for the key.
   Zone names are limited to 63 characters.

4. From the **Type** list, select **Key Signing Key**.

5. From the **State** list, select **Enabled**.

6. From the **Hardware Security Module** list, select **External**, if you use a network HSM.

7. From the **Algorithm** list, select the digest algorithm the system uses to generate the key signature.
   Your options are **RSA/SHA1**, **RSA/SHA256**, and **RSA/SHA512**.

8. From the **Key Management** list, select **Manual**.
   The Key Settings area displays **Certificate** and **Private Key** lists.

9. In the Key Settings area, select a certificate/key pair:
a) From the **Certificate** list, select a certificate.
b) From the **Private Key** list, select the key that matches the certificate you selected.

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

### Creating a DNSSEC zone

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

*Important:* The DNSSEC feature is available only when the BIG-IP system is licensed for BIG-IP DNS.

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

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

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

### Confirming that BIG-IP DNS is signing DNSSEC records

After you create DNSSEC zones and zone-signing keys, you can confirm that BIG-IP® DNS is signing the DNSSEC records.

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

### Configuring DNSSEC with an internal HSM

You can configure BIG-IP® DNS to use the DNSSEC protocol to secure the DNS traffic handled by BIG-IP DNS in conjunction with an internal HSM system.
Important: Before you configure DNSSEC, ensure that at least one data center and a server representing the BIG-IP DNS device exist in the BIG-IP system configuration.

**Task summary**
Perform these tasks to configure DNSSEC on BIG-IP DNS.

*Creating listeners to identify DNS traffic*

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

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

*Creating a DNSSEC zone*

*Confirming that BIG-IP DNS is signing DNSSEC records*

### 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.

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

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

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

- The amount of time required to send the DS records for the zone to which this key is associated to the organization that manages the parent zone.
- The value of the rollover period must be greater than half the value of the expiration period, as well as less than the value of the expiration period.
- The difference between the values of the rollover and expiration periods must be more than the value of the TTL.
Note: The values recommended in this procedure are based on the values in the NIST Secure Domain Name System (DNS) Deployment Guide.

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

1. On the Main tab, click DNS > Delivery > Keys > DNSSEC Key List.
   The DNSSEC Key List screen opens.
2. Click Create.
   The New DNSSEC Key screen opens.
3. In the Name field, type a name for the key.
   Zone names are limited to 63 characters.
4. From the Type list, select Zone Signing Key.
5. From the State list, select Enabled.
6. From the Hardware Security Module list, select Internal, if you use a FIPs internal HSM card.
7. From the Algorithm list, select the digest algorithm the system uses to generate the key signature.
   Your options are RSA/SHA1, RSA/SHA256, and RSA/SHA512.
8. From the Key Management list, select Automatic.
   The Key Settings area displays fields for key configuration.
9. In the Bit Width field, type 1024.
10. In the TTL field, accept the default value of 86400 (the number of seconds in one day.)

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

11. For the Rollover Period setting, in the Days field, type 21.
12. For the Expiration Period setting, in the Days field, type 30.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Creating a DNSSEC zone

Before you configure DNSSEC, ensure that at least one data center and a server object representing the
BIG-IP device exist in the BIG-IP system configuration.
**Important:** The DNSSEC feature is available only when the BIG-IP system is licensed for BIG-IP DNS.

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

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

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

### Confirming that BIG-IP DNS is signing DNSSEC records

After you create DNSSEC zones and zone-signing keys, you can confirm that BIG-IP® DNS is signing the DNSSEC records.

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

### About DNSSEC signing of zone transfers

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

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

**Important:** The DNSSEC feature is available only when a BIG-IP system is licensed for BIG-IP DNS (formerly GTM™).
Example of DNS Express signing zone transfers with DNSSEC keys

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

1. Creation of DNS zone initiates unsolicited zone transfer request for siterequest.com

   ![BIG-IP DNS configured with DNS zone with DNS Express server and DNSSEC zone for siterequest.com](image1)

   2. Unsolicited zone transfer sent to DNS Express and stored as unsigned zone.

   ![Authoritative DNS server](image2)

   Figure 10: Unsigned DNS zone transfer to DNS Express

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

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

   ![BIG-IP DNS configured with DNS zone with DNS Express server and DNSSEC zone for siterequest.com](image3)

   1. Upon zone update, NOTIFY message

   2. Zone transfer

   3. Zone transfer request for siterequest.com

   4. Unsigned zone stored in DNS Express

   5. NOTIFY message sent to client

   6. Zone transfer request for siterequest.com

   7. DNSSEC-signed zone transfer

   ![Authoritative DNS server](image4)

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

Important: The DNSSEC feature is available only when the BIG-IP system is licensed for BIG-IP DNS.
Example of DNS zone proxy with DNSSEC

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

![Diagram of DNS zone proxy with DNSSEC](image)

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

**Important:** The DNSSEC feature is available only when the BIG-IP system is licensed for BIG-IP DNS.

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

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

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

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

*Important: The DNSSEC feature is available only when the BIG-IP system is licensed for BIG-IP DNS.*

**Task summary**

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

- **Enabling BIG-IP to respond to zone transfer requests**
- **Enabling a DNS listener to process DNSSEC traffic**
- **Creating automatically managed DNSSEC zone-signing keys**
- **Creating manually managed DNSSEC zone-signing keys**
- **Creating automatically managed DNSSEC key-signing keys**
- **Creating manually managed DNSSEC key-signing keys**
- **Creating a DNSSEC zone**
- **Adding nameserver objects that represent DNS servers**
Enabling BIG-IP to respond to zone transfer requests

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

1. On the Main tab, click DNS > Delivery > Profiles > DNS. The DNS profile list screen opens.
2. Click Create. The New DNS Profile screen opens.
3. In the Name field, type a unique name for the profile.
4. Select the Custom check box.
5. In the DNS Traffic area, from the Zone Transfer list, select Enabled.
6. In the DNS Features area, from the Use BIND Server on BIG-IP list, select Disabled.
7. Click Finished.

Assign the profile to a listener.

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

Enabling a DNS listener to process DNSSEC traffic

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

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

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

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

1. On the Main tab, click DNS > Delivery > Listeners. The Listeners List screen opens.
2. Click the name of the listener you want to modify.
3. In the Service area, from the DNS Profile list, select the custom DNS profile with Zone Transfer enabled, and Use BIND server on BIG-IP disabled.
4. Click Finished.
5. Perform steps 2 - 4 to modify each of the other listeners.

Creating automatically managed DNSSEC zone-signing keys

Ensure that the time setting on BIG-IP® DNS is synchronized with the NTP servers on your network. This ensures that each BIG-IP DNS in a synchronization group is referencing the same time when generating keys.
Determine the values you want to configure for the rollover period, expiration period, and TTL of the keys, using the following criteria:

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

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

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

1. On the Main tab, click DNS > Delivery > Keys > DNSSEC Key List. The DNSSEC Key List screen opens.
2. Click Create. The New DNSSEC Key screen opens.
3. In the Name field, type a name for the key. Zone names are limited to 63 characters.
4. From the Type list, select Zone Signing Key.
5. From the State list, select Enabled.
6. From the Hardware Security Module list, select None.
7. From the Algorithm list, select the digest algorithm the system uses to generate the key signature. Your options are RSA/SHA1, RSA/SHA256, and RSA/SHA512.
8. From the Key Management list, select Automatic. The Key Settings area displays fields for key configuration.
9. In the Bit Width field, type 1024.
10. In the TTL field, accept the default value of 86400 (the number of seconds in one day.) This value specifies how long a client resolver can cache the key. This value must be less than the difference between the values of the rollover and expiration periods of the key; otherwise, a client can make a query and the system can send a valid key that the client cannot recognize.
11. For the Rollover Period setting, in the Days field, type 21.
12. For the Expiration Period setting, in the Days field, type 30. Zero seconds indicates not set, and thus the key does not expire.
13. For the Signature Validity Period setting, accept the default value of seven days. This value must be greater than the value of the signature publication period.
14. For the Signature Publication Period setting, accept the default value of four days and 16 hours. This value must be less than the value of the signature validity period.
15. Click Finished.
16. To create a standby key for emergency rollover purposes, repeat these steps using a similar name, and select Disabled from the State list.
Creating manually managed DNSSEC zone-signing keys

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

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

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

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

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

Creating automatically managed DNSSEC key-signing keys

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

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

- The amount of time required to send the DS records for the zone to which this key is associated to the organization that manages the parent zone.
- The value of the rollover period must be greater than half the value of the expiration period, as well as less than the value of the expiration period.
- The difference between the values of the rollover and expiration periods must be more than the value of the TTL.
Note: The values recommended in these steps are based on the values in the NIST Secure Domain Name System (DNS) Deployment Guide.

Create key-signing keys for BIG-IP DNS to use in the DNSSEC authentication process.

1. On the Main tab, click DNS > Delivery > Keys > DNSSEC Key List.
   The DNSSEC Key List screen opens.
2. Click Create.
   The New DNSSEC Key screen opens.
3. In the Name field, type a name for the key.
   Zone names are limited to 63 characters.
4. From the Type list, select Key Signing Key.
5. From the State list, select Enabled.
6. From the Hardware Security Module list, select None.
7. From the Algorithm list, select the digest algorithm the system uses to generate the key signature.
   Your options are RSA/SHA1, RSA/SHA256, and RSA/SHA512.
8. From the Key Management list, select Automatic.
   The Key Settings area displays fields for key configuration.
9. In the Bit Width field, type 2048.
10. In the TTL field, accept the default value of 86400 (the number of seconds in one day.)
    This value specifies how long a client resolver can cache the key. This value must be less than the
    difference between the values of the rollover and expiration periods of the key; otherwise, a client can
    make a query and the system can send a valid key that the client cannot recognize.
11. For the Rollover Period setting, in the Days field, type 340.
12. For the Expiration Period setting, in the Days field, type 365.
    Zero seconds indicates not set, and thus the key does not expire.
13. For the Signature Validity Period setting, accept the default value of seven days.
    This value must be greater than the value of the signature publication period.
    Zero seconds indicates not set, and thus the server verifying the signature never succeeds, because the
    signature is always expired.
14. For the Signature Publication Period setting, accept the default value of four days and 16 hours.
    This value must be less than the value of the signature validity period.
    Zero seconds indicates not set, and thus the signature is not cached.
15. Click Finished.
16. To create a standby key for emergency rollover purposes, repeat these steps using a similar name, and
    select Disabled from the State list.

Creating manually managed DNSSEC key-signing keys

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

When you plan to manually create keys, install the certificate and key pairs on the BIG-IP system, before
you attempt to create DNSSEC keys.
Importantly: Certificate and key file pairs must have the same name, for example, `exthsm.crt` and `exthsm.key`.

Create key-signing keys for BIG-IP DNS to use in the DNSSEC authentication process.

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

Creating a DNSSEC zone

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

**Important:** The DNSSEC feature is available only when the BIG-IP system is licensed for BIG-IP DNS.

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

1. On the Main tab, click **DNS > Zones > DNSSEC Zones.**
   The DNSSEC Zone List screen opens.
2. Click **Create.**
   The New DNSSEC Zone screen opens.
3. In the **Name** field, type a domain name.
   For example, use a zone name of `siterequest.com` to handle DNSSEC requests for `www.siterequest.com` and `*.www.siterequest.com`.
4. From the **State** list, select **Enabled.**
5. For the **Zone Signing Key** setting, assign at least one enabled zone-signing key to the zone.
   You can associate the same zone-signing key with multiple zones.
6. For the **Key Signing Key** setting, assign at least one enabled key-signing key to the zone.
   You can associate the same key-signing key with multiple zones.
7. Click **Finished.**
Adding nameserver objects that represent DNS servers

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

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

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

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

Adding nameserver objects that represent DNS nameservers (clients)

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

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

2. Click Create. The New Nameserver screen opens.
3. In the Name field, type a name for the DNS nameserver (client).
4. In the Address field, type the IP address on which the DNS nameserver (client) listens for DNS messages.
5. Optional: From the TSIG Key list, select the TSIG key you want the BIG-IP system to use to validate zone transfer traffic.
6. Click Finished.
7. Add nameserver objects to represent other DNS nameservers (clients).

Add the DNS nameservers (clients) objects to the Zone Transfer Client list of the DNS zone on the BIG-IP system.
Configuring a DNS zone to answer zone transfer requests

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

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

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

Viewing DNSSEC zone statistics

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

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

Troubleshooting DNSSEC on the BIG-IP system

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

**Task summary**

When you want to troubleshoot the DNSSEC configuration on BIG-IP DNS, perform these tasks.

*Accessing DNSSEC SEP records*

*Modifying generations of a DNSSEC key*

Accessing DNSSEC SEP records

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

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

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

### Modifying generations of a DNSSEC key

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

1. On the Main tab, click **DNS > Delivery > Keys > DNSSEC Key List**. The DNSSEC Key List screen opens.
2. Click a number in the Generations column. Information about this generation of the key displays.

<table>
<thead>
<tr>
<th>Column Title</th>
<th>Contains</th>
</tr>
</thead>
<tbody>
<tr>
<td>ID</td>
<td>Generation number of the key</td>
</tr>
<tr>
<td>Key Tag</td>
<td>Identifier (hash) of this generation of the key</td>
</tr>
<tr>
<td>Creator</td>
<td>Host name of BIG-IP DNS that created this generation of the key</td>
</tr>
<tr>
<td>Rollover Time</td>
<td>Time this generation of the key will roll over</td>
</tr>
<tr>
<td>Expiration Time</td>
<td>Time this generation of the key will expire</td>
</tr>
</tbody>
</table>

3. Click the number in the ID column. The general properties of the generation of the key display.
4. Select **Specify** from the **Rollover Time** list, and then select the exact time that you want the BIG-IP system to create and begin to use a new generation of this key. Modifying this setting does not affect the value of the rollover and expiration periods of the key.
5. Select **Specify** from the **Expiration Time** list, and then select the exact time that you want this generation of the key to expire. Modifying this setting does not affect the value of the rollover and expiration periods of the key.
6. Click **Update**.
Configuring DNS Caching

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

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

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

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

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

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

Important: The DNS Cache feature is available only when the BIG-IP system is licensed for DNS Services.

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

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

About the validating resolver DNS cache

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

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

Important: The DNS Cache feature is available only when the BIG-IP system is licensed for DNS Services.

About information stored in DNS caches

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

Message cache

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

Resource Record cache

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

Nameserver cache

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

Key cache

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

Configuring DNS cache global settings

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

1. On the Main tab, click System > Configuration > Local Traffic > DNS.

The DNS Local Traffic configuration screen opens.
2. In the **Minimum TTL** field, type the minimum number of seconds you want the system to cache DNS resource records.

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

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

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

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

   The default value for EDNS is **4096** bytes.

5. Click **Update**.

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

---

**Overview: Caching responses from external resolvers**

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

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

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

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

*Important:* The DNS Cache feature is available only when the BIG-IP system is licensed for DNS Services.
Configuring DNS Caching

Task summary

- Creating a transparent DNS cache
- Enabling transparent DNS caching
- Creating a custom DNS monitor
- Creating a pool of local DNS servers
- Determining DNS cache performance
- Clearing a DNS cache

Creating a transparent DNS cache

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

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

Associate the DNS cache with a custom DNS profile.
Enabling transparent DNS caching

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

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

1. On the Main tab, click **DNS > Delivery > Profiles > DNS** or **Local Traffic > Profiles > Services > DNS**.
   The DNS profile list screen opens.

2. Click **Create**.
   The New DNS Profile screen opens.

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

4. In the General Properties area, from the **Parent Profile** list, accept the default **dns** profile.

5. Select the **Custom** check box.

6. In the DNS Features area, from the **Use BIND Server on BIG-IP** list, select **Disabled**.

7. In the DNS Features area, from the **DNS Cache** list, select **Enabled**.
   When you enable the **DNS Cache** option, you must also select a DNS cache from the **DNS Cache Name** list.

8. In the DNS Features area, from the **DNS Cache Name** list, select the DNS cache that you want to associate with this profile.
   You can associate a DNS cache with a profile, even when the **DNS Cache** option, is **Disabled**.

9. Click **Finished**.

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

Creating a custom DNS monitor

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

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

1. On the Main tab, click **DNS > Delivery > Load Balancing > Monitors** or **Local Traffic > Monitors**.
   The Monitor List screen opens.

2. Click **Create**.
   The New Monitor screen opens.

3. Type a name for the monitor in the **Name** field.

4. From the **Type** list, select **DNS**.

5. In the **Query Name** field, type the domain name that you want the monitor to query.
   For the zone, siterequest.com, you might want the monitor to query for www.siterequest.com.

6. Configure additional settings based on your network requirements.

7. Click **Finished**.
Creating a pool of local DNS servers

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

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

1. On the Main tab, click 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**.

Determining DNS cache performance

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

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

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

   The DNS Caches Status Summary screen opens.

2. From the **Statistics Type** list, select **Caches**.

   Information displays about the DNS caches.

<table>
<thead>
<tr>
<th>Record type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Queries</td>
<td>Total number of queries handled by the cache.</td>
</tr>
<tr>
<td>Responses</td>
<td>Total number of responses sent from the cache.</td>
</tr>
<tr>
<td>Sync</td>
<td>Number of synchronous queries handled by the cache.</td>
</tr>
<tr>
<td>Async</td>
<td>Number of asynchronous queries handled by the cache.</td>
</tr>
<tr>
<td>Resolve</td>
<td>Total number of DNS resolve failures.</td>
</tr>
<tr>
<td>Connect</td>
<td>Total number of DNS connect failures.</td>
</tr>
<tr>
<td>Server</td>
<td>Number of DNS server failures.</td>
</tr>
</tbody>
</table>
3. In the Details column for a cache, click View to display detailed information about the cache.
4. To return to the DNS Cache Statistics screen, click the Back button.

**Viewing records in a DNS cache**

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

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

3. At the tmsh prompt, type the command:
   
   show ltm dns cache records rrset cache <cache name>

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

**Viewing DNS cache statistics**

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

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

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

**Viewing DNS cache statistics using tmsh**

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

   The DNS Caches Status Summary screen opens.
2. From the Statistics Type list, select Caches.
   Information displays about the DNS caches.

<table>
<thead>
<tr>
<th>Record type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Queries</td>
<td>Total number of queries handled by the cache.</td>
</tr>
<tr>
<td>Responses</td>
<td>Total number of responses sent from the cache.</td>
</tr>
<tr>
<td>Sync</td>
<td>Number of synchronous queries handled by the cache.</td>
</tr>
<tr>
<td>Async</td>
<td>Number of asynchronous queries handled by the cache.</td>
</tr>
<tr>
<td>Resolve</td>
<td>Total number of DNS resolve failures.</td>
</tr>
<tr>
<td>Record type</td>
<td>Description</td>
</tr>
<tr>
<td>-------------</td>
<td>------------------------------</td>
</tr>
<tr>
<td>Connect</td>
<td>Total number of DNS connect failures.</td>
</tr>
<tr>
<td>Server</td>
<td>Number of DNS server failures.</td>
</tr>
<tr>
<td>Send</td>
<td>Number of DNS response send failures.</td>
</tr>
</tbody>
</table>

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

**Managing transparent cache size**

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

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

1. On the Main tab, click **DNS > Caches > Cache List**.
   The DNS Cache List screen opens.
2. Click the name of the cache you want to modify.
   The properties screen opens.
3. In the **Message Cache Size** field, type the maximum size in bytes for the DNS message cache.
   The BIG-IP system caches the messages in a DNS response in the message cache. A higher maximum size makes it possible for more DNS responses to be cached and increases the cache hit percentage. A lower maximum size forces earlier eviction of cached content, but can lower the cache hit percentage.
   
   **Important:** When you change the value of the **Message Cache Size**, the records in the message cache are automatically removed. If you do not want to clear the message cache, do not change the value of this parameter.

4. In the **Resource Record Cache Size** field, type the maximum size in bytes for the DNS resource record cache.
   The BIG-IP system caches the supporting records in a DNS response in the Resource Record cache. A higher maximum size makes it possible for more DNS responses to be cached and increases the cache hit percentage. A lower maximum size forces earlier eviction of cached content, but can lower the cache hit percentage.
   
   **Warning:** When you change the value of the **Resource Record Cache Size**, the records in the resource record cache are automatically removed from the cache. If you do not want to clear the resource record cache, do not change the value of this parameter.

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

6. Click Finished.

**Clearing a DNS cache**

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

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

Clearing groups of records from a DNS cache

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

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

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>To clear messages from the cache:</td>
<td>change the value in the Message Cache Size field.</td>
</tr>
<tr>
<td>To clear resource records from the cache:</td>
<td>change the value in the Resource Record Cache Size field.</td>
</tr>
<tr>
<td>To clear nameservers from the cache:</td>
<td>change the value in the Name Server Cache Count field.</td>
</tr>
<tr>
<td>To clear DNSSEC keys from the cache:</td>
<td>change the value in the DNSSEC Key Cache Size field.</td>
</tr>
</tbody>
</table>

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

Clearing specific records from a DNS cache using tmsh

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

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

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

Overview: Resolving queries and caching responses

You can configure the BIG-IP® system to resolve DNS queries and cache the responses by creating a resolver DNS cache. The next time the BIG-IP system receives a query for a response that exists in the cache, the system returns the response from the cache. The resolver cache contains messages, resource records, and the nameservers the system queries to resolve DNS queries.
**Important:** The DNS Cache feature is available only when the BIG-IP system is licensed for DNS Services.

**Task summary**
- Creating a resolver DNS cache
- Enabling resolving and caching
- Determining DNS cache performance
- Clearing a DNS cache
Creating a resolver DNS cache

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

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

Associate the DNS cache with a custom DNS profile.

Enabling resolving and caching

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

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

1. On the Main tab, click DNS or Local Traffic > Profiles > DNS.
   The DNS profile list screen opens.
2. Click Create.
   The New DNS Profile screen opens.
3. In the Name field, type a unique name for the profile.
4. Select the Custom check box.
5. In the DNS Features area, from the Use BIND Server on BIG-IP list, select Disabled.
6. In the DNS Features area, from the DNS Cache list, select Enabled.
   When you enable the DNS Cache option, you must also select a DNS cache from the DNS Cache Name list.
7. In the DNS Features area, from the DNS Cache Name list, select the DNS cache that you want to associate with this profile.
   You can associate a DNS cache with a profile, even when the DNS Cache option is Disabled.
8. Click Finished.

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

Determining DNS cache performance

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

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

   The DNS Caches Summary screen opens.
2. From the Statistics Type list, select Caches.
   Information displays about the DNS caches.
### Viewing records in a DNS cache

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

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

### Viewing DNS cache statistics

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

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

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

### Viewing DNS cache statistics using tmsh

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

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

### Configuring DNS Caching

<table>
<thead>
<tr>
<th>Record type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Queries</td>
<td>Total number of queries handled by the cache.</td>
</tr>
<tr>
<td>Responses</td>
<td>Total number of responses sent from the cache.</td>
</tr>
<tr>
<td>Sync</td>
<td>Number of synchronous queries handled by the cache.</td>
</tr>
<tr>
<td>Async</td>
<td>Number of asynchronous queries handled by the cache.</td>
</tr>
<tr>
<td>Resolve</td>
<td>Total number of DNS resolve failures.</td>
</tr>
<tr>
<td>Connect</td>
<td>Total number of DNS connect failures.</td>
</tr>
<tr>
<td>Server</td>
<td>Number of DNS server failures.</td>
</tr>
<tr>
<td>Send</td>
<td>Number of DNS response send failures.</td>
</tr>
</tbody>
</table>
### Record type and Description

<table>
<thead>
<tr>
<th>Record type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Queries</td>
<td>Total number of queries handled by the cache.</td>
</tr>
<tr>
<td>Responses</td>
<td>Total number of responses sent from the cache.</td>
</tr>
<tr>
<td>Sync</td>
<td>Number of synchronous queries handled by the cache.</td>
</tr>
<tr>
<td>Async</td>
<td>Number of asynchronous queries handled by the cache.</td>
</tr>
<tr>
<td>Resolve</td>
<td>Total number of DNS resolve failures.</td>
</tr>
<tr>
<td>Connect</td>
<td>Total number of DNS connect failures.</td>
</tr>
<tr>
<td>Server</td>
<td>Number of DNS server failures.</td>
</tr>
<tr>
<td>Send</td>
<td>Number of DNS response send failures.</td>
</tr>
</tbody>
</table>

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

### Managing cache size

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

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

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

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

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

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

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

   **Important:** When you change the value of the **Nameserver Cache Count**, the records in the nameserver cache are automatically removed from the cache. If you do not want to clear the nameserver cache, do not change the value of this parameter.
6. In the **Unsolicited Reply Threshold** field, change the default value if you are using the BIG-IP® system to monitor for unsolicited replies using SNMP.

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

7. Click **Update**.

### Clearing a DNS cache

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

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

2. On the menu bar, click **Statistics**.
   
   The Local Traffic Statistics screen opens.

3. Select the check box next to the cache you want to clear, and then click **Clear Cache**.

### Clearing groups of records from a DNS cache

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

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

2. Click the name of the cache you want to modify.
   
   The properties screen opens.

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

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

4. Click **Update**.
   
   The BIG-IP® system clears the records in the caches that you resized.

### Clearing specific records from a DNS cache using tmsh

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

---

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

---

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

   `tmsh`
3. At the tmsh prompt, to navigate to the directory that contains the DNS cache records, type the command:

   ltm dns cache records

4. To delete specific DNS cache records, type a variation of this command:

   delete <cache-type> type <record-type> cache <cache-name>

   For example, the command delete rrset type a cache my Resolver_cache, deletes the A records from the resource record cache of the resolver cache named my Resolver_cache.

---

**Overview: Resolving queries and caching validated responses**

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

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

**Important:** The DNS Cache feature is available only when the BIG-IP system is licensed for DNS Services.
Creating a validating resolver DNS cache

Create a validating resolver cache on the BIG-IP® system when you want the system to resolve DNS queries, use DNSSEC to validate the responses, and cache the responses.
1. On the Main tab, click DNS > Caches > Cache List.  
The DNS Cache List screen opens.

2. Click Create.  
The New DNS Cache screen opens.

3. In the Name field, type a name for the cache.

4. From the Resolver Type list, select Validating Resolver.

5. Click Finished.

Associate the DNS cache with a custom DNS profile.

### About SEP records and DNSSEC

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

### Obtaining a trust or DLV anchor

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

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

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

2. Click the name of the DNSSEC zone for which you want to view or copy SEP records.

3. On the menu bar, click SEP Records.  
The SEP records display for each generation of a key. If the SEP record screen is unexpectedly blank, ensure that at least one data center and a server representing the BIG-IP DNS device exist in the BIG-IP system configuration.

4. Copy the trust or DLV anchor from the DNSKEY Record field.

### Adding a trust anchor to a validating resolver DNS cache

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

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

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

2. Click the name of the cache you want to modify.  
The properties screen opens.

3. On the menu bar, click Trust Anchors.  
The Trust Anchors screen opens.

4. Click the Add button.

5. In the Trust Anchor field, paste the trust anchor that you copied from the signed zone.

---

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

6. Click Finished.

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

The validating resolver can now validate the content of DNS responses from the zones for which you added trust anchors.
Adding a DLV anchor to a validating resolver DNS cache

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

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

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

   **Important: The DLV anchor must be specified in a string format.**
6. Click **Finished**.
7. For each additional DLV anchor that you want to add to the validating resolver, repeat steps 4-6.

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

Enabling validating resolver DNS caching

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

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

1. On the Main tab, click **DNS > Delivery > Profiles > DNS or Local Traffic > Profiles > Services > DNS**.
   The DNS profile list screen opens.
2. Click **Create**.
   The New DNS Profile screen opens.
3. In the **Name** field, type a unique name for the profile.
4. In the General Properties area, from the **Parent Profile** list, accept the default **dns** profile.
5. Select the **Custom** check box.
6. In the DNS Features area, from the **Use BIND Server on BIG-IP** list, select **Disabled**.
7. In the DNS Features area, from the **DNS Cache** list, select **Enabled**.
   When you enable the **DNS Cache** option, you must also select a DNS cache from the **DNS Cache Name** list.
8. In the DNS Features area, from the **DNS Cache Name** list, select the DNS cache that you want to associate with this profile.
   You can associate a DNS cache with a profile, even when the **DNS Cache** option, is **Disabled**.
9. Click **Finished**.

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

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

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


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

<table>
<thead>
<tr>
<th>Record type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Queries</td>
<td>Total number of queries handled by the cache.</td>
</tr>
<tr>
<td>Responses</td>
<td>Total number of responses sent from the cache.</td>
</tr>
<tr>
<td>Sync</td>
<td>Number of synchronous queries handled by the cache.</td>
</tr>
<tr>
<td>Async</td>
<td>Number of asynchronous queries handled by the cache.</td>
</tr>
<tr>
<td>Resolve</td>
<td>Total number of DNS resolve failures.</td>
</tr>
<tr>
<td>Connect</td>
<td>Total number of DNS connect failures.</td>
</tr>
<tr>
<td>Server</td>
<td>Number of DNS server failures.</td>
</tr>
<tr>
<td>Send</td>
<td>Number of DNS response send failures.</td>
</tr>
</tbody>
</table>

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

Viewing records in a DNS cache

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

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

3. At the `tmsh` prompt, type the command:
   
   `show ltm dns cache records rrset cache <cache name>`

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

Viewing DNS cache statistics

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

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

2. From the Statistics Type list, select Caches.
3. In the Details column for a cache, click View to display detailed information about the cache.
4. To return to the DNS Cache Statistics screen, click the Back button.

**Viewing DNS cache statistics using tmsh**

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

   The DNS Caches Status Summary screen opens.
2. From the Statistics Type list, select Caches.
   Information displays about the DNS caches.

<table>
<thead>
<tr>
<th>Record type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Queries</td>
<td>Total number of queries handled by the cache.</td>
</tr>
<tr>
<td>Responses</td>
<td>Total number of responses sent from the cache.</td>
</tr>
<tr>
<td>Sync</td>
<td>Number of synchronous queries handled by the cache.</td>
</tr>
<tr>
<td>Async</td>
<td>Number of asynchronous queries handled by the cache.</td>
</tr>
<tr>
<td>Resolve</td>
<td>Total number of DNS resolve failures.</td>
</tr>
<tr>
<td>Connect</td>
<td>Total number of DNS connect failures.</td>
</tr>
<tr>
<td>Server</td>
<td>Number of DNS server failures.</td>
</tr>
<tr>
<td>Send</td>
<td>Number of DNS response send failures.</td>
</tr>
</tbody>
</table>

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

**Managing cache size**

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

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

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

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

4. In the Resource Record Cache Size field, type the maximum size in bytes for the DNS resource record cache.
   The BIG-IP system caches the supporting records in a DNS response in the Resource Record cache. A higher maximum size makes it possible for more DNS responses to be cached and increases the cache hit percentage. A lower maximum size forces earlier eviction of cached content, but can lower the cache hit percentage.
Warning: When you change the value of the Resource Record Cache Size, the records in the resource record cache are automatically removed from the cache. If you do not want to clear the resource record cache, do not change the value of this parameter.

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

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

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

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

7. Click Update.

Clearing a DNS cache

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

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

Clearing groups of records from a DNS cache

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

1. On the Main tab, click DNS > Caches > Cache List.
   The DNS Cache List screen opens.
2. Click the name of the cache you want to modify.
   The properties screen opens.
3. In the DNS Cache area, to clear specific records from the cache, do one of the following:
   
<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>To clear messages from the cache:</td>
<td>change the value in the Message Cache Size field.</td>
</tr>
<tr>
<td>To clear resource records from the cache:</td>
<td>change the value in the Resource Record Cache Size field.</td>
</tr>
<tr>
<td>To clear nameservers from the cache:</td>
<td>change the value in the Name Server Cache Count field.</td>
</tr>
<tr>
<td>To clear DNSSEC keys from the cache:</td>
<td>change the value in the DNSSEC Key Cache Size field.</td>
</tr>
</tbody>
</table>

4. Click Update.

The BIG-IP® system clears the records in the caches that you resized.
Clearing specific records from a DNS cache using tmsh

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

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

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

Overview: Resolving queries for local zones with authoritative responses

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

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

![Client](image.png)

Figure 17: Successful DNS query resolution from transparent local zone
About local zones

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

Adding local zones to a DNS cache

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

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

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

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

1. On the Main tab, click DNS > Caches > Cache List. The DNS Cache List screen opens.
2. Click the name of the cache you want to modify. The properties screen opens.
3. On the menu bar, click Local Zones. The Local Zones screen opens.
4. Click the Add button.
5. In the Name field, type the domain name of the local zone.
   
   Note: The domain you enter must be at the apex of the zone. For example, you could name a local zone siterequest.com, and then add resource records for the members wiki.siterequest.com and download.siterequest.com.

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

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

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Deny</td>
<td>For a non-matching query, the cache drops the DNS query.</td>
</tr>
<tr>
<td>Option</td>
<td>Description</td>
</tr>
<tr>
<td>---------</td>
<td>-------------</td>
</tr>
</tbody>
</table>
| **Redirect** | For a non-matching query, when the query is for a subdomain of the local zone, the cache returns the same response that it would for the local zone. For example, if you add the local zone `siterequest.com`, the cache returns the same response to queries for `wiki.siterequest.com` and `download.wiki.siterequest.com`.

This is an example of a response to a non-matching query: **NOERROR** rcode returned and `example.com. NOT resolved as expected` |
| **Refuse** | For a non-matching query, the cache returns a REFUSED message in the DNS response.  

This is an example of a response to a non-matching query: **REFUSED** rcode returned and `example.com. NOT resolved as expected` |
| **Static** | For a non-matching query, the cache returns a NoData or NXDOMAIN in the DNS response, which also includes the SOA record if the local zone contains one.  

This is an example of a response to a non-matching query: **NOERROR** rcode returned and `example.com. NOT resolved as expected` |
| **Transparent** | **Transparent** is the default value.  

For a non-matching query, the cache performs a pass-through or iterative resolution of the DNS query. If the query matches, but no resource records are available, the cache returns a response with a NoData message.  

This is an example of a response to a non-matching query: **NOERROR** rcode returned and `example.com. NOT resolved as expected` |

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

   **Note:** You can add multiple resource records.

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

8. Click **Finished**.

---

**Overview: Forwarding specific DNS queries to specific nameservers**

You can configure a resolver or validating resolver DNS cache with forward zones. Do this configuration when you want the BIG-IP system to forward DNS queries that match the forward zones to specific nameservers, which resolve the query when the cache does not contain a response.
For example, the network administrator for Site Request wants to configure the DNS cache to resolve responses to queries for the zone: `app1.siterequest.com`. She wants the responses to queries for this zone to be served from specific nameservers, when the cache does not contain a response.

![Figure 19: Successful DNS query resolution from forward zone](image)

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

### About forward zones

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

### Longest match

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

### Selecting a nameserver

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

### Task summary

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

*Adding forward zones to a DNS cache*
Adding forward zones to a DNS cache

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

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

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

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

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

7. Click Finished.

Deleting forward zones from a DNS cache

Determine which forward zone you want to delete.

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

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

Changing the nameservers associated with a forward zone

Determine the forward zone that you want to modify.

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

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

**Viewing statistics about DNS cache forward zones**

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

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

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

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

You can configure a resolver or validating resolver DNS cache with a forward zone that is associated with a listener. The listener can load balance specific DNS queries to a pool of DNS servers. For example, the network administrator for SiteRequest wants to configure the DNS cache to resolve DNS queries for the forward zone `app2.siterequest.com`, and wants the responses to be served from a pool of local DNS servers, when the cache does not contain a response.

![Figure 20: Successful DNS query resolution from pool of DNS servers associated with a forward zone](image)

**Task summary**

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

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

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

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

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

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

1. On the Main tab, click 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 a resolver DNS cache

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

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

Associate the DNS cache with a custom DNS profile.

Enabling resolving and caching

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

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

1. On the Main tab, click DNS > Delivery > Profiles > DNS or Local Traffic > Profiles > Services > DNS.
   The DNS profile list screen opens.
2. Click Create.
   The New DNS Profile screen opens.
3. In the Name field, type a unique name for the profile.
4. Select the Custom check box.
5. In the DNS Features area, from the Use BIND Server on BIG-IP list, select Disabled.
6. In the DNS Features area, from the DNS Cache list, select Enabled.
   When you enable the DNS Cache option, you must also select a DNS cache from the DNS Cache Name list.
7. In the DNS Features area, from the DNS Cache Name list, select the DNS cache that you want to associate with this profile.
   You can associate a DNS cache with a profile, even when the DNS Cache option is Disabled.
8. Click Finished.

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

Creating listeners that alert 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.

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

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

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

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

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

7. Click Finished.

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

Overview: Customizing a DNS cache

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

- Resolving DNS queries for default local zones from a DNS cache
- Using specific DNS servers as authoritative root nameservers
- Alerting the system to cache poisoning
- Configuring RRset Rotate to specify the order to return resource records

**Resolving DNS queries for default local zones from a DNS cache**

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

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

*Overview: Customizing a DNS cache*

**Using specific DNS servers as authoritative root nameservers**

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

1. On the Main tab, click **DNS > Caches > Cache List**. The DNS Cache List screen opens.
2. Click the name of the cache you want to modify. The properties screen opens.
3. In the Root Hints area, in the **IP address** field, type the IP address of a DNS server that the system considers authoritative for the DNS root nameservers, and then click **Add**.

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

4. Click **Update**.

*Overview: Customizing a DNS cache*

**Alerting the system to cache poisoning**

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

1. On the Main tab, click **DNS > Caches > Cache List**. The DNS Cache List screen opens.
2. Click the name of the cache you want to modify. The properties screen opens.
3. In the **Unsolicited Reply Threshold** field, change the default value if you are using the BIG-IP system to monitor for unsolicited replies using SNMP.
The system always rejects unsolicited replies. The default value of 0 (off) indicates the system does not generate SNMP traps or log messages when rejecting unsolicited replies. Changing the default value alerts you to a potential security attack, such as cache poisoning or DOS. For example, if you specify 1,000,000 unsolicited replies, each time the system receives 1,000,000 unsolicited replies, it generates an SNMP trap and log message.

4. Click **Update**.

**Overview: Customizing a DNS cache**

### Configuring RRset Rotate to specify the order to return resource records

You can configure which method the DNS cache uses on the BIG-IP® system when deciding the order to return resource records within cached responses.

1. On the Main tab, click **DNS > Caches > Cache List**.
   The DNS Cache List screen opens.
2. Click the name of the cache you want to modify.
   The properties screen opens.
3. In the DNS Cache area, for the **RRSet Rotate** field, select one of the following options:

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>none (default)</td>
<td>Returns resource records in the same order as received.</td>
</tr>
<tr>
<td>query id</td>
<td>Uses the query identification number to decide which resource record to set first.</td>
</tr>
</tbody>
</table>

*Note: The rotation methodology used is based on picking a random number to select the first entry of the Resource Record Set (RRset). Local zones that are part of a Response Policy Zone are not rotated.*

4. Click **Update**.

**Overview: Customizing a DNS cache**
Configuring DNS Response Policy Zones

Overview: DNS response policy zones and the BIG-IP system

The BIG-IP® system can utilize a domain name service (DNS) response policy zone (RPZ) as a firewall mechanism. An RPZ is a zone that contains a list of known malicious Internet domains. The list includes a resource record set (RRset) for each malicious domain. Each RRset includes the names of the malicious domain and any subdomains of the domain.

When the BIG-IP system receives a DNS query for a domain that is on the malicious domain list of the RPZ, the system responds in one of two ways based on your configuration. You can configure the system to return an NXDOMAIN record that indicates that the domain does not exist.

**Figure 21: BIG-IP returns NXDOMAIN response to DNS query for malicious domain**

Alternatively, you can configure the system to return the response that directs the user to a walled garden.

**Figure 22: BIG-IP forwards DNS query for malicious domain to walled garden**

About creating an RPZ using ZoneRunner

There are a number of vendors that host response policy zones (RPZs). The BIG-IP® system supports RPZ vendors. F5® has tested the BIG-IP system with the vendors Spamhaus (http://www.spamhaus.org/organization/dnsblusage/) and SURBL (http://www.surbl.org/df). If you do not want to purchase a subscription from a vendor, you can use ZoneRunner® on the BIG-IP system to create a custom RPZ.

**Note:** ZoneRunner is available only with a BIG-IP DNS license.

Task summary

*Creating a custom RPZ using ZoneRunner*

*Adding resource records to a custom RPZ*

Creating a custom RPZ using ZoneRunner

Determine the host name and IP address of the BIG-IP® system on which you are configuring the RPZ.
You can create your own RPZ when you do not want to subscribe to an RPZ vendor.

1. On the Main tab, click DNS > Zones > ZoneRunner > Zone List.
   The Zone List screen opens.
2. Click Create.
   The New Zone screen opens.
3. From the View Name list, select external.
   The external view is a default view to which you can assign zones.
4. In the Zone Name field, type a name for the zone file.
   For example, to replicate the format of Spamhaus and SURBL DSN RPZ names, type rpz.myblacklist.org
5. From the Zone Type list, select Master.
6. Clear the Zone File Name field, and type the zone file name.
   db.external.rpz.blacklist.org
7. In the Options field, add an also-notify statement to ensure that BIND notifies DNS Express when
   the zone is updated; for example: also-notify { ::1 port 5353; };
8. In the SOA Record section, type values for the record fields:
   a) In the TTL field, type the default time-to-live (TTL) for the records in the zone.
   b) In the Master Server field, type the name of the BIG-IP DNS on which you are configuring this
      zone.
9. In the NS Record section, type values for the record fields:
   a) In the TTL field, type the time-to-live (TTL) for the nameserver record.
   b) In the NameServer field, type the name of the BIG-IP DNS on which you are configuring this
      zone.
10. Click Finished.
    Add resource records that represent known malicious domains to your custom RPZ.

Adding resource records to a custom RPZ

Determine the names of the known malicious domain names that you want to include in your custom
DNS response policy zone (RPZ).

For each malicious domain that you want to add to your custom RPZ, create a resource record for the
domain. Additionally, you can add a wildcard resource record to represent all subdomains of the
malicious domain.

1. On the Main tab, click DNS > Zones > ZoneRunner > Zone List.
   The Zone List screen opens.
2. Click the name of a custom RPZ to which you want to add malicious zone names.
   The Zone Properties screen opens.
3. Click Add Resource Record.
   The New Resource Record screen opens.
4. In the Name field, type the name of the malicious domain in front of the RPZ zone name that
   displays: [zone_name].rpz.myblacklist.org.
   maliciouszone.com.rpz.myblacklist.org. for the domain name or
5. In the TTL field, type the time-to-live (TTL) for the CNAME record.
6. From the **Type** list, select **CNAME**.
7. In the **CNAME** field, type .
8. Click **Finished**.
9. Create additional resource records for each malicious domain that you want to include in your customer RPZ. Remember to create a resource record for the domain and a resource record for the subdomains.

You can now implement your RPZ on the BIG-IP system or on an external name server.

**About configuring the BIG-IP system to use an RPZ as a DNS firewall**

With an RPZ configuration, the BIG-IP® system filters DNS queries for domains that are known to be malicious and returns custom responses that direct those queries away from the malicious domain.

**Task summary**

*Optional: Adding a TSIG key for the server that hosts the RPZ*

*Adding a nameserver object for the server that hosts the RPZ*

*Creating an RPZ DNS Express zone*

*Creating a DNS cache*

*Adding a local zone to represent a walled garden*

*Adding an RPZ to a DNS cache*

*Staging the RPZ on your network*

*Creating a custom DNS profile for DNS caching*

*Viewing DNS zone statistics*

*Viewing DNS cache statistics*

**Optional: Adding a TSIG key for the server that hosts the RPZ**

Before adding a TSIG key for a DNS server that hosts an RPZ:

- Ensure that the DNS server is configured to allow the BIG-IP® system to perform zone transfers.
- Ensure that the time on the systems that use TSIG keys are synchronized.
- Obtain the TSIG key for each DNS server.

Add a TSIG key to the BIG-IP system configuration, when you want to validate zone transfer communications between DNS Express® and a DNS server hosting an RPZ.

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

Add the TSIG key to the DNS nameserver that represents the RPZ on the BIG-IP system.

**Adding a nameserver object for the server that hosts the RPZ**

Obtain the IP address of the authoritative DNS server that hosts the DNS response policy zone (RPZ).
When you want to transfer an RPZ from an authoritative DNS server into the DNS Express® engine, add a nameserver object that represents the server that hosts the zone.

1. On the Main tab, click DNS > Delivery > Nameservers.
   The Nameservers List screen opens.
2. Click Create.
   The New Nameserver screen opens.
3. In the Name field, type a name for the authoritative DNS server.
4. In the Address field, type the IP address on which the DNS server listens for DNS messages.
   If the RPZ is hosted on BIND on the BIG-IP system, use the name localhost and the default Address 127.0.0.1 and Service Port 53.
5. From the TSIG Key list, select the TSIG key that matches the TSIG key on this DNS server.
   The BIG-IP system uses this TSIG key to sign zone transfer requests to the DNS server hosting the zone.
6. Click Finished.

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

Creating an RPZ DNS Express zone

Before you create the DNS Express zone:

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

__Note: Zone names are case insensitive.__

Create a DNS Express zone on the BIG-IP® system when you want to transfer an RPZ into DNS Express.

1. On the Main tab, click DNS > Zones.
   The Zone List screen opens.
2. Click Create.
   The New Zone screen opens.
3. In the Name field, type the name of the DNS zone.
   The name must begin and end with a letter and contain only letters, numbers, and the period and hyphen (-) characters.
4. In the DNS Express area, from the Server list, select the authoritative primary DNS server that currently hosts the zone.
   __Note: The DNS Express engine requests zone transfers from this server.__
5. Select the Response Policy check box.
6. Click Finished.

Creating a DNS cache

Ensure that the global DNS settings are configured based on your network architecture.

Create a DNS cache on the BIG-IP® system when you want to utilize an RPZ to protect your network from known malicious domains.
1. On the Main tab, click **DNS > Caches > Cache List.**
   The DNS Cache List screen opens.

2. Click **Create.**
   The New DNS Cache screen opens.

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

4. From the **Resolver Type** list, select one of three types:

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Resolver</td>
<td>Resolves a DNS request and stores the response in the DNS cache.</td>
</tr>
<tr>
<td>Validating Resolver</td>
<td>Resolves a DNS request, verifies the response using a DNSSEC key, and</td>
</tr>
</tbody>
</table>
<pre><code>             | stores the response in the DNS cache.                                     |
</code></pre>
<p>| Transparent (None)   | Sends a DNS request to a DNS server for resolution, and stores the response |
| in the DNS cache.                                                         |</p>

5. Click **Finished.**

### Adding a local zone to represent a walled garden

Ensure that a DNS cache with which you are implementing the RPZ is configured on the BIG-IP® system.

Obtain the resource records for the walled garden zone on your network.

When you want the BIG-IP system to redirect DNS queries for known malicious domains to a specific domain, add a local zone that represents a walled garden on your network to the DNS cache you will use to implement an RPZ.

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

2. Click the name of the cache you want to modify.
   The properties screen opens.

3. On the menu bar, click **Local Zones.**
   The Local Zones screen opens.

4. Click the **Add** button.

5. In the **Name** field, type the domain name of the walled garden on your network.

   **Note:** The domain you enter must be the exact name you want to use for the walled garden. Ensure that you use a zone name that does not match any other resources on your network, for example, `walledgarden.siterequest.com`.

6. From the **Type** list, select **Static.**

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

   For example, if the local zone name is `walledgarden.siterequest.com`, then this is an example of an A record entry: `walledgarden.siterequest.com. IN A 10.10.10.124`, and this is an example of a AAAA record entry: `walledgarden.siterequest.com. IN AAAA 2002:0:1:12:123:c:cd:cdf`.

8. Click **Finished.**

### Adding an RPZ to a DNS cache

If you want the BIG-IP® system to redirect DNS queries for known malicious domains to a specific location, ensure that you have associated a local zone that represents the RPZ with the DNS cache.
Add an RPZ to a DNS cache on the BIG-IP® system when you want to protect your network from known malicious domains.

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

2. Click the name of the cache you just created.
   
The properties screen opens.

3. On the menu bar, click **Response Policy Zones.**
   
The Response Policy Zones screen opens.

4. Click the Add button.

5. From the Zone list, select an RPZ.

6. From the Action list, select an action:

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>NXDOMAIN</td>
<td>Resolves a DNS query for a malicious domain found in the RPZ with an NXDOMAIN response, which states that the domain does not exist.</td>
</tr>
<tr>
<td>walled-garden</td>
<td>Resolves a DNS query for a malicious domain found in the RPZ by providing an A or AAAA record response, which redirects the query to a known host.</td>
</tr>
</tbody>
</table>

7. If you selected the type Walled Garden, from the **Walled Garden IP** list, select the local zone that represents the walled garden on your network.

8. Click **Finished.**

### Staging the RPZ on your network

Ensure that a DNS cache configured with an RPZ exists on the system.

When you want to test how using an RPZ affects your network environment, modify the RPZ by enabling the **Logs and Stats Only** setting.

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

2. Click the name of the cache you want to modify.
   
The properties screen opens.

3. On the menu bar, click **Response Policy Zones.**
   
The Response Policy Zones screen opens.

4. Click the name of the RPZ you want to modify.

5. Select the **Logs and Stats Only** check box.

   When checked, queries that match a malicious domain in the RPZ list are logged and statistics are created; however, RPZ policies are not enforced. That is, when a DNS query matches a malicious domain in the RPZ list, the system does not return an NXDOMAIN response or redirect the query to a walled garden.

   **Warning:**

   System performance is affected even when **Logs and Stats Only** is selected. This is because the system still performs RPZ lookups.

6. Click **Finished.**

### Creating a custom DNS profile for DNS caching

Ensure that at least one DNS cache exists on the BIG-IP® system.
You can create a custom DNS profile to configure the BIG-IP system to cache responses to DNS queries.

1. On the Main tab, click **Local Traffic > Profiles > Services > DNS**. The DNS profile list screen opens.
2. Click **Create**. The New DNS Profile screen opens.
3. In the **Name** field, type a unique name for the profile.
4. In the General Properties area, from the **Parent Profile** list, accept the default dns profile.
5. Select the **Custom** check box.
6. In the DNS Features area, from the **DNS Cache** list, select **Enabled**. When you enable the DNS Cache option, you must also select a DNS cache from the DNS Cache Name list.
7. In the DNS Features area, from the **DNS Cache Name** list, select the DNS cache that you want to associate with this profile.
   You can associate a DNS cache with a profile, even when the DNS Cache option, is **Disabled**.
8. Click **Finished**.

**Viewing DNS zone statistics**

You can view information about DNS zones.

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

**Viewing DNS cache statistics**

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

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

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

**About configuring the BIG-IP system as an RPZ distribution point**

You can configure an RPZ on the BIG-IP® system and allow other nameservers to perform zone transfers of the RPZ.

*Warning:* DNS Express® supports only full zone transfers (AXFRs); therefore, transferring an RPZ from the BIG-IP system to another nameserver creates additional traffic on your internal network.
Task summary

Configuring the BIG-IP system as a distribution point for an RPZ
Enabling the BIG-IP system to respond to zone transfer requests

Configuring the BIG-IP system as a distribution point for an RPZ

Ensure that you have created a DNS Express zone for the RPZ.

Enable the DNS Express zone for the RPZ to be a distribution point on your network to allow other nameservers to perform zone transfers of the RPZ.

1. On the Main tab, click DNS > Zones.
   The Zone List screen opens.
2. Click the name of the zone you want to modify.
3. In the Zone Transfer Clients area, move the nameservers that can initiate zone transfers from the Available list to the Active list.
4. Optional: From the TSIG Key list, select the TSIG key you want the BIG-IP system to use to validate zone transfer traffic.
5. Click Update.

Enabling the BIG-IP system to respond to zone transfer requests

To enable the BIG-IP system to respond to zone transfer requests for an RPZ zone, create a custom DNS profile.

1. On the Main tab, click DNS > Delivery > Profiles > DNS.
   The DNS profile list screen opens.
2. Click Create.
   The New DNS Profile screen opens.
3. In the General Properties area, name the profile dns_zxfr.
4. Select the Custom check box.
5. In the DNS Traffic area, from the Zone Transfer list, select Enabled.
6. Click Finished.
Overview: Configuring DNS64

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

Note: When you are configuring DNS64, in addition to the BIG-IP DNS license, the system requires both CGNAT and DNS services licenses.

Task summary

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

Creating a custom DNS profile

Before you start, make sure that you have activated licenses for BIG-IP® DNS, and both the CGNAT and DNS services.

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

1. On the Main tab, click DNS > Delivery > Profiles > DNS or Local Traffic > Profiles > Services > DNS.
   The DNS profile list screen opens.

2. Click Create.
   The New DNS Profile screen opens.
3. In the Name field, type a unique name for the profile.
4. In the General Properties area, from the Parent Profile list, accept the default dns profile.
5. Select the Custom check box.
6. In the DNS Features area, from the GSLB list, accept the default value Enabled.
7. In the DNS Features area, from the DNS IPv6 to IPv4 list, select how you want the system to handle IPv6 to IPv4 address mapping in DNS queries and responses.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Disabled</td>
<td>The BIG-IP system does not map IPv4 addresses to IPv6 addresses.</td>
</tr>
<tr>
<td>Immediate</td>
<td>The BIG-IP system receives an AAAA query and forwards the query to a DNS server. The BIG-IP system then forwards the first good response from the DNS server to the client. If the system receives an A response first, it appends a 96-bit prefix to the record and forwards it to the client. If the system receives an AAAA response first, it simply forwards the response to the client. The system disregards the second response from the DNS server.</td>
</tr>
<tr>
<td>Secondary</td>
<td>The BIG-IP system receives an AAAA query and forwards the query to a DNS server. Only if the server fails to return a response does the BIG-IP system send an A query. If the BIG-IP system receives an A response, it appends a 96-bit user-configured prefix to the record and forwards it to the client.</td>
</tr>
<tr>
<td>V4 Only</td>
<td>The BIG-IP system receives an AAAA query, but forwards an A query to a DNS server. After receiving an A response from the server, the BIG-IP system appends a 96-bit user-configured prefix to the record and forwards it to the client.</td>
</tr>
</tbody>
</table>

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

If you selected Immediate, Secondary, or V4 Only two new fields display.
8. In the DNS Features area, in the IPv6 to IPv4 Prefix field, specify the prefix the BIG-IP system appends to all A query responses to an IPv6 request.
9. In the DNS Features area, from the IPv6 to IPv4 Additional Section Rewrite list, select an option to allow improved network efficiency for both Unicast and Multicast DNS-SD responses.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Disabled</td>
<td>The BIG-IP system does not perform additional rewrite.</td>
</tr>
<tr>
<td>V4 Only</td>
<td>The BIG-IP system accepts only A records. The system appends the 96-bit user-configured prefix to a record and returns an IPv6 response to the client.</td>
</tr>
<tr>
<td>V6 Only</td>
<td>The BIG-IP system accepts only AAAA records and returns an IPv6 response to the client.</td>
</tr>
<tr>
<td>Any</td>
<td>The BIG-IP system accepts and returns both A and AAAA records. If the DNS server returns an A record in the Additional section of a DNS message, the BIG-IP system appends the 96-bit user-configured prefix to the record and returns an IPv6 response to the client.</td>
</tr>
</tbody>
</table>

10. In the DNS Features area, from the Use BIND Server on BIG-IP list, select Enabled.

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

11. Click Finished.

Assigning a DNS profile to a DNS listener
1. On the Main tab, click **DNS > Delivery > Listeners.**  
   The Listeners List screen opens.
2. Click the name of the listener you want to modify.
3. In the Service area, from the **DNS Profile** list, select the profile you created to manage IPv6 to IPv4 address mapping.
4. Click **Update.**
   
   This listener can now pass traffic between an IPv6-only client and an IPv4-only DNS server.

**Implementation result**

You now have an implementation of DNS64 on the BIG-IP® system.
Configuring IP Anycast (Route Health Injection)

Overview: Configuring IP Anycast (Route Health Injection)

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

Task Summary

- Enabling the ZebOS dynamic routing protocol
- Creating a custom DNS profile
- Configuring a listener for route advertisement
- Verifying advertisement of the route

Enabling the ZebOS dynamic routing protocol

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

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

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

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

Creating a custom DNS profile

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

1. On the Main tab, click DNS > Delivery > Profiles > DNS.
   The DNS profile list screen opens.
2. Click Create.
   The New DNS Profile screen opens.
3. In the Name field, type a unique name for the profile.
4. In the General Properties area, from the Parent Profile list, accept the default dns profile.
5. Select the **Custom** check box.
6. In the DNS Features area, from the **GSLB** list, accept the default value **Enabled**.
7. In the DNS Features area, from the **Unhandled Query Actions** list, select how you want the BIG-IP system to handle a query that is not for a wide IP or DNS Express zone.

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

8. In the DNS Features area, from the **Use BIND Server on BIG-IP** list, select **Enabled**.

---

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

9. Click **Finished**.

### Configuring a listener for route advertisement

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

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

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

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

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

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>dns</td>
<td>This is the default DNS profile. With the default dns profile, BIG-IP DNS forwards non-wide IP queries to the BIND server on the BIG-IP DNS system itself.</td>
</tr>
<tr>
<td>&lt;custom profile&gt;</td>
<td>If you have created a custom DNS profile to handle non-wide IP queries in a way that works for your network configuration, select it.</td>
</tr>
</tbody>
</table>

10. Click **Finished**.
Verifying advertisement of the route

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

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

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

Implementation result

You now have an implementation in which the BIG-IP® system broadcasts virtual IP addresses that you configured for route advertisement.
Configuring IP Anycast (Route Health Injection)
Configuring Remote High-Speed DNS Logging

Overview: Configuring remote high-speed DNS logging

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

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

![Diagram showing the association of configuration objects for remote high-speed logging]

Figure 24: Association of remote high-speed logging configuration objects

Task summary

Creating a pool of remote logging servers
Creating a remote high-speed log destination
Creating a formatted remote high-speed log destination
Creating a publisher
Creating a custom DNS logging profile for logging DNS queries
Creating a custom DNS logging profile for logging DNS responses
Creating a custom DNS logging profile for logging DNS queries and responses
Creating a custom DNS profile to enable DNS logging
Configuring logs for global server load-balancing decisions
Disabling DNS logging

About the configuration objects of remote high-speed DNS logging

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

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

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

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

1. On the Main tab, click the applicable path.
   • DNS > Delivery > Load Balancing > Pools
   • Local Traffic > Pools
   The Pool List screen opens.

2. Click Create.
   The New Pool screen opens.

3. In the Name field, type a unique name for the pool.

4. Using the New Members setting, add the IP address for each remote logging server that you want to include in the pool:
   a) Type an IP address in the Address field, or select a node address from the Node List.
   b) Type a service number in the Service Port field, or select a service name from the list.
   
   Note: Typical remote logging servers require port 514.

   c) Click Add.

5. Click Finished.

Creating a remote high-speed log destination

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

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

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

2. Click Create.

3. In the Name field, type a unique, identifiable name for this destination.

4. From the Type list, select Remote High-Speed Log.

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

   The BIG-IP system is configured to send an unformatted string of text to the log servers.

5. From the Pool Name list, select the pool of remote log servers to which you want the BIG-IP system to send log messages.

6. From the Protocol list, select the protocol used by the high-speed logging pool members.

7. Click Finished.
Creating a formatted remote high-speed log destination

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

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

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

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

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

   **Important:** For logs coming from Access Policy Manager® (APM®), only the BSD Syslog format is supported.
6. If you selected Splunk or IPFIX, from the Forward To list, select the destination that points to a pool of high-speed log servers to which you want the BIG-IP system to send log messages.
7. Click Finished.

Creating a publisher

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

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

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

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

Creating a custom DNS logging profile for logging DNS queries

Create a custom DNS logging profile to log DNS queries, when you want to log only DNS queries.
1. On the Main tab, click **DNS > Delivery > Profiles > Other > DNS Logging** or **Local Traffic > Profiles > Other > DNS Logging**.  
The DNS Logging profile list screen opens.

2. Click **Create**.  
The New DNS Logging profile screen opens.

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

4. From the **Log Publisher** list, select a destination to which the BIG-IP system sends DNS log entries.

5. For the **Log Queries** setting, ensure that the **Enabled** check box is selected, if you want the BIG-IP system to log all DNS queries.

6. For the **Include Query ID** setting, select the **Enabled** check box, if you want the BIG-IP system to include the query ID sent by the client in the log messages.

7. Click **Finished**.  
Assign this custom DNS logging profile to a custom DNS profile.

---

### Creating a custom DNS logging profile for logging DNS responses

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

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

2. Click **Create**.  
The New DNS Logging profile screen opens.

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

4. From the **Log Publisher** list, select a destination to which the BIG-IP system sends DNS log entries.

5. For the **Log Responses** setting, select the **Enabled** check box, if you want the BIG-IP system to log all DNS responses.

6. For the **Include Query ID** setting, select the **Enabled** check box, if you want the BIG-IP system to include the query ID sent by the client in the log messages.

7. Click **Finished**.  
Assign this custom DNS logging profile to a custom DNS profile.

---

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

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

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

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

2. Click **Create**.  
The New DNS Logging profile screen opens.

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

4. From the **Log Publisher** list, select a destination to which the BIG-IP system sends DNS log entries.

5. For the **Log Queries** setting, ensure that the **Enabled** check box is selected, if you want the BIG-IP system to log all DNS queries.
6. For the **Log Responses** setting, select the **Enabled** check box, if you want the BIG-IP system to log all DNS responses.

7. For the **Include Query ID** setting, select the **Enabled** check box, if you want the BIG-IP system to include the query ID sent by the client in the log messages.

8. Click **Finished**.

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

---

### Creating a custom DNS profile to enable DNS logging

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

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

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

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

---

### Configuring 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.

<table>
<thead>
<tr>
<th>Check-box option</th>
<th>Log information</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Pool Selection</strong></td>
<td>The pool selected to answer a DNS request, and why the pool was selected.</td>
</tr>
<tr>
<td><strong>Pool Traversal</strong></td>
<td>The pools in the wide IP considered during the load-balancing decision, and why the pool was selected.</td>
</tr>
<tr>
<td><strong>Pool Member Selection</strong></td>
<td>The pool member selected to answer a DNS request, and why the member was selected.</td>
</tr>
</tbody>
</table>
Check-box option | Log information
---|---
Pool Member | The members of the pool considered during the load-balancing decision, and why the member was selected.
Traversal | 

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)]

**Disabling DNS logging**

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

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

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

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

**Implementation result**

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

Overview: Setting up and viewing DNS statistics

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

DNS AVR Statistics

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

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

DNS Global Statistics

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

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

Task Summary

Creating a DNS profile for AVR statistics collection
Configuring a BIG-IP DNS listener for DNS AVR statistics collection
Viewing DNS AVR statistics
Viewing DNS AVR statistics in tmsh
Viewing DNS global statistics
Viewing DNS statistics for a specific virtual server

Creating a DNS profile for AVR statistics collection

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

Configure the BIG-IP® system to collect AVR statistics on a sampling of the DNS traffic that the BIG-IP system handles.
1. On the Main tab, click **DNS** > **Delivery** > **Profiles** > **DNS** or **Local Traffic** > **Profiles** > **Services** > **DNS**.
   The DNS profile list screen opens.

2. Click **Create**.
   The New DNS Profile screen opens.

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

4. Select the **Custom** check box.

5. In the Logging and Reporting area, select the **AVR Statistics Sample Rate** check box.
   The **Enabled 1/1 queries sampled** field displays.

6. In the **Enabled 1/1 queries sample** field, change the 1 to the number of queries from which the system takes one sample.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>No DNS requests are stored in the Analytics database.</td>
</tr>
<tr>
<td>1</td>
<td>All DNS requests are stored in the Analytics database.</td>
</tr>
<tr>
<td>n&gt;1</td>
<td>Every nth DNS request is stored in the Analytics database.</td>
</tr>
</tbody>
</table>

7. Click **Finished**.
   Assign the DNS profile to a listener or virtual server.

**Configuring a BIG-IP DNS listener for DNS AVR statistics collection**

Ensure that at least one custom DNS profile configured with an AVR sampling rate exists on the BIG-IP® system.

Assign a custom DNS profile to a listener when you want the BIG-IP system to collect AVR statistics on a sampling of the DNS traffic the listener handles.

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

1. On the Main tab, click **DNS** > **Delivery** > **Listeners**.
   The Listeners List screen opens.

2. Click the name of the listener you want to modify.

3. In the Service area, from the **DNS Profile** list, select a custom DNS profile configured with an AVR sampling rate.

4. Click **Update**.

**Viewing DNS AVR statistics**

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

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

1. On the Main tab, click **Statistics** > **Analytics** > **DNS**.
   The DNS Analytics screen opens.

2. From the **View By** list, select the specific network object type for which you want to display statistics.
   You can also click **Expand Advanced Filters** to filter the information that displays.

3. From the **Time Period** list, select the amount of time for which you want to view statistics.

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

4. Click **Export** to create a report of this information.
**Viewing DNS AVR statistics in tmsh**

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

View DNS analytics data to help you manage the DNS traffic on your network.

1. Log on to the command-line interface of the BIG-IP system.
2. At the BASH prompt, type `tmsh`.
3. At the `tmsh` prompt, type one of these commands and then press Enter.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>show analytics dns report view-by query-name limit 3</code></td>
<td>Displays the three most common query names.</td>
</tr>
<tr>
<td><code>show analytics dns report view-by query-type limit 3</code></td>
<td>Displays the three most common query types.</td>
</tr>
<tr>
<td><code>show analytics dns report view-by client-ip limit 3</code></td>
<td>Displays the three client IP addresses from which the most DNS queries originate.</td>
</tr>
<tr>
<td><code>show analytics dns report view-by query-name drilldown { { entity query-type values {A}}} limit 3</code></td>
<td>Displays the three most common query names for query type A records.</td>
</tr>
<tr>
<td><code>show analytics dns report view-by query-type drilldown { { entity query-name values {www.f5.com}}} limit 3</code></td>
<td>Displays the three most common query types for query name <code>www.f5.com</code>.</td>
</tr>
<tr>
<td><code>show analytics dns report view-by client-ip drilldown { { entity query-type values {A}}} limit 3</code></td>
<td>Displays the three most common client IP addresses requesting query type A records.</td>
</tr>
</tbody>
</table>

**Viewing DNS global statistics**

Ensure that at least one DNS profile exists on the BIG-IP® system and that this profile is assigned to an LTM® virtual server or a DNS listener that is configured to use the TCP protocol.

*Note: If you want to view AXFR and IXFR statistics, the listener or virtual server must be configured to use the TCP protocol. This is because zone transfers occur over the TCP protocol.*

View DNS global statistics to determine how to fine-tune your network configuration or troubleshoot DNS traffic processing problems.

2. From the **Statistics Type** list, select **Profiles**.
3. In the Global Profile Statistics area, in the Details column of the DNS profile, click **View**.

**Viewing DNS statistics for a specific virtual server**

Ensure that at least one virtual server associated with a DNS profile exists on the BIG-IP® system.
Note: If you want to view AXFR and IXFR statistics, the virtual server must be configured to use the TCP protocol. This is because zone transfers occur over the TCP protocol.

You can view DNS statistics per virtual server when you want to analyze how the BIG-IP system is handling specific DNS traffic.

   The Local Traffic statistics screen opens.
2. From the Statistics Type list, select Virtual Servers.
3. In the Details column for the virtual server, click View.

Implementation result

You now have an implementation in which the BIG-IP® system gathers both DNS AVR and DNS global statistics. You can view these statistics to help you understand DNS traffic patterns and manage the flow of your DNS traffic, especially when your network is under a DDoS attack.
Using ZoneRunner to Configure DNS Zones

About ZoneRunner

You can use the ZoneRunner™ utility to create and manage DNS zone files and configure the BIND instance on BIG-IP® DNS (formerly GTM™). With the ZoneRunner utility, you can:

- Import and transfer DNS zone files
- Manage zone resource records
- Manage views
- Manage a local nameserver and the associated configuration file, named.conf
- Transfer zone files to a nameserver
- Import only primary zone files from a nameserver

About named.conf

named.conf contains the primary operational characteristics of BIND, including DNS views, access control list definitions, and zones. The ZoneRunner™ utility updates named.conf when you modify the local BIND instance.

Using ZoneRunner to configure named.conf

Ensure that at least one zone is configured on BIG-IP® DNS.

Use ZoneRunner™ to edit named.conf, to decrease the risk of a syntax error that prevents the BIND system from performing as expected. Zonerunner provides an automatic syntax check and displays error messages to help you write the correct syntax.

1. On the Main tab, click DNS > Zones > ZoneRunner > named Configuration.
   The named Configuration screen opens.
2. In the Options area, type additional configurations per your network design.
3. Click Update.

Creating a master DNS zone

A master zone is authoritative. Create a zone when you want to use ZoneRunner™ to manage DNS zones and resource records.

Tip: The BIG-IP® system can be either a primary or secondary DNS server.

1. On the Main tab, click DNS > Zones > ZoneRunner > Zone List.
   The Zone List screen opens.
2. Click Create.
   The New Zone screen opens.
3. From the View Name list, select external.
   The external view is a default view to which you can assign zones.
4. In the Zone Name field, type a period character (.).
5. From the Zone Type list, select Master.
6. Clear the Zone File Name field, and type the zone file name.
Creating a hint zone

*Hint zones* designate a subset of the root nameservers list. When the local nameserver starts (or restarts), the nameserver queries the root servers in the hint zone for the most current list of root servers. The root hint is built into BIND version 9.0 and later.

Create a zone when you want to use ZoneRunner™ to manage DNS zones and resource records.

**Tip:** The BIG-IP® system can be either a primary or secondary DNS server.

1. On the Main tab, click **DNS > Zones > ZoneRunner > Zone List.**
   The Zone List screen opens.
2. Click **Create.**
   The New Zone screen opens.
3. From the **View Name** list, select **external.**
   The external view is a default view to which you can assign zones.
4. In the **Zone Name** field, type a period character (.).
5. From the **Zone Type** list, select **Hint.**
6. Clear the **Zone File Name** field, and type the zone file name.
   
   ```
   db.external.siterequest.com
   
   Note: Do not include a trailing dot.
   ```
7. Click **Finished.**
   If you want further help creating a custom hint file, see SOL8380 on www.askf5.com for instructions.

Configuring BIG-IP DNS to allow zone file transfers

By default, BIG-IP® DNS is configured to secure BIND to not allow zone transfers except from the localhost. However, you can configure BIG-IP DNS to allow zone file transfers to other DNS servers.

1. On the Main tab, click **DNS > Zones > ZoneRunner > named Configuration.**
   The named Configuration screen opens.
2. In the **Options** field, modify the allow-transfer statement to include the IP address of the BIG-IP DNS.
   You can modify the following allow-transfer statement to use the IP address of the BIG-IP DNS.

```plaintext
allow-transfer {
    localhost;
    192.168.10.105;
};
```
3. On the menu bar, click **View List.**
   The View List screen opens.
4. Click the name of the view that contains the zone you are configuring.
The View Configuration screen opens.

5. In the Options area, modify the match-clients statement based on your configuration.

<table>
<thead>
<tr>
<th>View configuration type</th>
<th>Add to match-clients statement</th>
</tr>
</thead>
</table>
| Single view configuration | view "external" {  
  match-clients {  
    "zrd-acl-000-000";  
    any;  
  };  
} |

<table>
<thead>
<tr>
<th>Multiple view configuration</th>
<th>Modify the following match-clients statement to use the IP address of the BIG-IP DNS.</th>
</tr>
</thead>
</table>
| where you want to allow transfers from BIG-IP DNS | acl "internal-acl"  
  { <IP address> ;  
  };  
view "internal" {  
  match-clients {  
    "zrd-acl-000-001";  
    "internal-acl";  
    <IP address> ;  
  };  
}  
view "external" {  
  match-clients {  
    "zrd-acl-000-000";  
    any;  
  };  
} |

6. Click Update.

To verify that zone transfers are working properly, modify this Linux command and run it on an external computer:

```sh
dig @<IP address> es.net. axfr
```

The command should return a response similar to this:

```sh
; <<>> DiG? 9.5.0-P2 <<>> @192.17.1.253 es.net. axfr
; (1 server found)
;; global options: printcmd
es.net. 500 IN SOA siterequest.com.
hostmaster.siterequest.com. 6 10800 3600 604800 60
es.net. 500 IN NS siterequest.com.
a.es.net. 30 IN A 192.17.1.100
b.es.net. 30 IN A 192.18.1.100
es.net. 500 IN SOA siterequest.com.
hostmaster.siterequest.com. 6 10800 3600 604800 60
;; Query time: 6 msec
;; SERVER: 192.17.1.253#53(192.17.1.253)
;; WHEN: Fri Mar 11 17:20:25 2011
;; XFR size: 5 records (messages 1, bytes 180)
```
About DNS views

A DNS view is a modification of a nameserver configuration based on the community attempting to access it. Using views, you can build multiple nameserver configurations on the same server, and have those configurations apply dynamically when the request originates from a specified source.

If your DNS handles requests from both inside and outside your company, you can create two views: internal and external.

Creating a DNS view

It is helpful to keep in mind that ZoneRunner™ contains a default view named: external.

Create an additional DNS view to modify the local nameserver configuration to allow a specific community to access it.

1. On the Main tab, click DNS > Zones > ZoneRunner > View List.
   The View List screen opens.
2. Click Create.
3. In the View Name field, type a name for the view.
4. From the View Order list, make a selection.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>First</td>
<td>In the view hierarchy, this view is listed first.</td>
</tr>
<tr>
<td>Last</td>
<td>In the view hierarchy, this view is listed last.</td>
</tr>
<tr>
<td>After</td>
<td>In the view hierarchy, this view is listed immediately following the view that you select from the View List.</td>
</tr>
</tbody>
</table>

5. In the Options area, modify the match-clients statement based on your configuration.

<table>
<thead>
<tr>
<th>View configuration type</th>
<th>Add to match-clients statement</th>
</tr>
</thead>
<tbody>
<tr>
<td>Single view configuration</td>
<td>view &quot;external&quot; {</td>
</tr>
<tr>
<td></td>
<td>match-clients {</td>
</tr>
<tr>
<td></td>
<td>&quot;zrd-acl-000-000&quot;;</td>
</tr>
<tr>
<td></td>
<td>any;</td>
</tr>
<tr>
<td></td>
<td>};</td>
</tr>
<tr>
<td>Multiple view configuration, where you want to allow transfers from BIG-IP DNS</td>
<td>Modify the following match-clients statement to use the IP address of the BIG-IP DNS.</td>
</tr>
<tr>
<td></td>
<td>acl &quot;internal-acl&quot; {</td>
</tr>
<tr>
<td></td>
<td>{ &lt;IP address&gt; ;</td>
</tr>
<tr>
<td></td>
<td>}</td>
</tr>
<tr>
<td></td>
<td>};</td>
</tr>
<tr>
<td></td>
<td>view &quot;internal&quot; {</td>
</tr>
<tr>
<td></td>
<td>match-clients {</td>
</tr>
<tr>
<td></td>
<td>&quot;zrd-acl-000-001&quot;;</td>
</tr>
<tr>
<td></td>
<td>&quot;internal-acl&quot;;</td>
</tr>
<tr>
<td></td>
<td>&lt;IP address&gt; ;</td>
</tr>
<tr>
<td></td>
<td>}</td>
</tr>
<tr>
<td></td>
<td>};</td>
</tr>
<tr>
<td></td>
<td>view &quot;external&quot; {</td>
</tr>
<tr>
<td></td>
<td>match-clients {</td>
</tr>
<tr>
<td></td>
<td>&quot;zrd-acl-000-000&quot;;</td>
</tr>
<tr>
<td></td>
<td>any;</td>
</tr>
<tr>
<td></td>
<td>}</td>
</tr>
<tr>
<td></td>
<td>};</td>
</tr>
</tbody>
</table>

6. In the Options area, type additional configurations per your network design.
7. Click **Finished**.

**Types of DNS zone files**

This table describes the types of DNS zone files.

<table>
<thead>
<tr>
<th>DNS file type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Primary</td>
<td>Zone files for a primary zone contain, at minimum, the start of authority (SOA) and nameserver (NS) resource records for the zone. Primary zones are authoritative, that is, they respond to DNS queries for the domain or sub-domain. A zone can have only one SOA record, and must have at least one NS record.</td>
</tr>
<tr>
<td>Secondary</td>
<td>Zone files for a secondary zone are copies of the principal zone files. At an interval specified in the SOA record, secondary zones query the primary zone to check for and obtain updated zone data. A secondary zone responds authoritatively for the zone provided that the zone data is valid.</td>
</tr>
<tr>
<td>Stub</td>
<td>Stub zones are similar to secondary zones, except that stub zones contain only the NS records for the zone. Note that stub zones are a specific feature of the BIND implementation of DNS. F5 Networks recommends that you use stub zones only if you have a specific requirement for this functionality.</td>
</tr>
<tr>
<td>Forward</td>
<td>The zone file for a forwarding zone contains only information to forward DNS queries to another nameserver on a per-zone (or per-domain) basis.</td>
</tr>
<tr>
<td>Hint</td>
<td>The zone file for a hint zone specifies an initial set of root nameservers for the zone. Whenever the local nameserver starts, it queries a root nameserver in the hint zone file to obtain the most recent list of root nameservers. Zone file import.</td>
</tr>
</tbody>
</table>

**Types of DNS resource records**

This table describes the types of DNS resource records that ZoneRunner™ supports.

<table>
<thead>
<tr>
<th>DNS file type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>SOA (Start of authority)</td>
<td>The start of authority resource record, SOA, starts every zone file and indicates that a nameserver is the best source of information for a particular zone. The SOA record indicates that a nameserver is authoritative for a zone. There must be exactly one SOA record per zone. Unlike other resource records, you create a SOA record only when you create a new master zone file.</td>
</tr>
<tr>
<td>A (Address)</td>
<td>The Address record, or A record, lists the IP address for a given host name. The name field is the host’s name, and the address is the network interface address. There should be one A record for each IP address of the machine.</td>
</tr>
<tr>
<td>AAAA (IPv6 Address)</td>
<td>The IPv6 Address record, or AAAA record, lists the 128-bit IPv6 address for a given host name.</td>
</tr>
<tr>
<td>CNAME (Canonical Name)</td>
<td>The Canonical Name resource record, CNAME, specifies an alias or nickname for the official, or canonical, host name. This record must be the only one associated with the alias name. It is usually easier to supply one A record for a given address and use CNAME records to define alias host names for that address.</td>
</tr>
<tr>
<td>DNAME (Delegation of Reverse Name)</td>
<td>The Delegation of Reverse Name resource record, DNAME, specifies the reverse lookup of an IPv6 address. These records substitute the suffix of one domain name with another. The DNAME record instructs DNS (BIG-IP® DNS, formerly GTM) (or any DNS server) to build an alias that substitutes a portion of the requested IP address with the data stored in the DNAME record.</td>
</tr>
<tr>
<td>DNS file type</td>
<td>Description</td>
</tr>
<tr>
<td>--------------------</td>
<td>--------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>HINFO (Host</td>
<td>The Host Information resource record, HINFO, contains information on the hardware and operating system relevant to BIG-IP DNS (formerly GTM) (or other DNS).</td>
</tr>
<tr>
<td>Information)</td>
<td></td>
</tr>
<tr>
<td>MX (Mail Exchanger)</td>
<td>The Mail Exchange resource record, MX, defines the mail system(s) for a given domain.</td>
</tr>
<tr>
<td>NAPTR (Name</td>
<td>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.</td>
</tr>
<tr>
<td>Authority Pointer)</td>
<td></td>
</tr>
<tr>
<td>NS (nameserver)</td>
<td>The nameserver resource record, NS, defines the nameservers for a given domain, creating a delegation point and a subzone. The first name field specifies the zone that is served by the nameserver that is specified in the nameservers name field. Every zone needs at least one nameserver.</td>
</tr>
<tr>
<td>PTR (Pointer)</td>
<td>A name pointer resource record, PTR, associates a host name with a given IP address. These records are used for reverse name lookups.</td>
</tr>
<tr>
<td>SRV (Service)</td>
<td>The Service resource record, SRV, is a pointer with which an alias for a given service is redirected to another domain. For example, if the fictional company Site Request has an FTP archive hosted on archive.siterequest.com, the IT department can create an SRV record with which the alias ftp.siterequest.com is redirected to archive.siterequest.com.</td>
</tr>
<tr>
<td>TXT (Text)</td>
<td>The Text resource record, TXT, allows you to supply any string of information, such as the location of a server or any other relevant information that you want available.</td>
</tr>
</tbody>
</table>
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, the BIG-IP system 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.

<table>
<thead>
<tr>
<th>Statistic type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Effective Rate Limit (RPS)</td>
<td>The number of DNS name resolution requests per second the BIG-IP system handles based on the rate-limited license installed on the system.</td>
</tr>
<tr>
<td>Object Count</td>
<td>The sum of these objects configured on the BIG-IP system: DNS Express® zones, DNS cache resolvers, and DNSSEC zones.</td>
</tr>
<tr>
<td>Rate Rejects</td>
<td>The number of DNS requests that the BIG-IP system has rejected based on the rate limit of the license installed on the system.</td>
</tr>
</tbody>
</table>

5. In the Global Traffic Management area, view the **Effective Rate Limit (RPS)**, **Object Count**, and **Rate Rejects** statistics.

<table>
<thead>
<tr>
<th>Statistic type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Effective Rate Limit (RPS)</td>
<td>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.</td>
</tr>
<tr>
<td>Object Count</td>
<td>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.</td>
</tr>
<tr>
<td>Rate Rejects</td>
<td>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.</td>
</tr>
</tbody>
</table>

**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 statistic is displayed.
<table>
<thead>
<tr>
<th>Statistic type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Rejects</td>
<td><em>Rejects</em> count for DNS increments, rather than the <em>Rate Rejects</em> count for Global Traffic Management incrementing.</td>
</tr>
</tbody>
</table>
Legal Notices

Legal notices

Publication Date
This document was published on May 8, 2018.

Publication Number
MAN-0533-02

Copyright
Copyright © 2017, F5 Networks, Inc. All rights reserved.

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

Trademarks
For a current list of F5 trademarks and service marks, see http://www.f5.com/about/guidelines-policies/trademarks.

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

Patents
This product may be protected by one or more patents indicated at: https://f5.com/about-us/policies/patents.

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

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

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

**Canadian Regulatory Compliance**

This Class A digital apparatus complies with Canadian ICES-003.

**Standards Compliance**

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

A

address mapping, about IPv6 to IPv4 105
allow-transfer statement
modifying for zone transfers 12
allow-transfer statement, modifying for zone file transfers 25, 31
also-notify statement
sending NOTIFY message from local BIND to DNS Express 12
Analytics
and viewing DNS statistics 122
and viewing DNS statistics in tmsh 123
creating profile for DNS AVR statistics collection 121
Anycast, See IP Anycast.
Application Visibility and Reporting (AVR)
and DNS statistics collection 121
and viewing DNS statistics 122
creating profile for DNS AVR statistics collection 121
AVR, and viewing DNS statistics 122

B

BIG-IP DNS
about rate-limited license statistics 131
BIG-IP system
configured as authoritative DNS server 9
configured as secondary DNS server 9
bitstream
enabling 21

C

cache clearing
and groups of records 73, 78, 85
using tmsh 73, 78, 86
cache poisoning, and configuring SNMP alerts 95
cache size, managing 77, 84
caching
and DNS profiles 102
caching, and DNS profiles 69, 75, 82, 93
custom DNS profiles
and disabling DNS logging 119
and enabling DNS Express 15
and enabling DNS zone transfers 18, 104
and enabling high-speed DNS logging 118
and logging DNS queries and responses 116, 117
creating 109
creating to enable DNSSEC signing of zone transfers 57
enabling zone transfers 27, 33
custom DNS profiles, and caching DNS responses 69
custom monitors, creating DNS 33, 69, 92

D

destinations
for logging 116
destinations (continued)
for remote high-speed logging 115
DLV anchors
and adding to validating resolvers 82
obtaining for validating resolvers 38, 81
DNS
adding nameservers (clients) to BIG-IP 17, 62
DNS AVR statistics
and listeners 122
overview 121
DNS cache
about 65
about configuring for specific needs 94
about forward zones 89
about resolver 65, 73
about transparent 67
about validating resolver 66, 79
adding an RPZ 100, 101
adding local zones 101
and adding DLV anchors to validating resolvers 82
and adding trust anchors to validating resolvers 81
and BIG-IP virtual servers as nameservers for a forward zone 94
and BIG-IP virtual servers as nameservers for forward zones 91
and creating validating resolvers 80
and deleting nameservers associated with a forward zone 90
and forward zones 88, 91
and forwarding requests to a local zone 87
and local zones 86, 88
and modifying forward zones 90
and obtaining trust and DLV anchors for validating resolvers 38, 81
and statistics for forward zones 91
clearing 72, 73, 78, 85, 86
clearing groups of records 73, 78, 85
configuring RRSet Rotate 96
configuring to alert for cache poisoning 95
configuring to answer DNS queries for default local zones 95
configuring to answer DNS queries for local static zones 87
configuring to generate SNMP alerts 95
configuring to use specific root nameservers 95
configuring transparent 65
creating resolver 75, 93
creating transparent 68
forward zones
about 89
managing cache size 77, 84
managing transparent cache size 72
viewing 71, 76, 83
viewing statistics 70, 71, 75, 76, 83, 103
viewing statistics using tmsh 71, 76, 84
DNS cache forwarder
deleting 90
DNS cache profiles
Index

DNS cache profiles (continued)            · customizing to cache DNS responses 69, 75, 82, 93
DNS caches                                   · adding 90
DNS Express                                  · about 9
                                                · about answering DNS queries 10
                                                · about answering zone transfer queries 10
                                                · about configuring 9
                                                · about zone transfer requests 17
                                                · acting as secondary authoritative DNS server 10, 17
                                                · acting as slave DNS server 10
                                                · and authoritative DNS servers 13, 62
                                                · and DNSSEC security 54
                                                · and handling NOTIFY messages without TSIG HMAC
                                                · and listeners 15
                                                · and NOTIFY messages from local BIND 12
                                                · and zone transfer requests 18
                                                · enabling 15
DNS Express zone                             · creating an RPZ 100
                                                · configuring as an RPZ distribution point 104
DNS fast path                                · about 19
DNS firewall                                  · and RPZs on the BIG-IP system 99
DNS global settings, configuring 66
DNS global statistics, overview 121
DNS high-speed logging                        · configuring 114
DNS high-speed logging, overview 113
DNS Logging                                   · disabling 119
                                                · enabling 118
DNS logging profiles, customizing 116, 117
DNS monitor, creating 33, 69, 92
DNS profiles                                  · and disabling DNS logging 119
                                                · and enabling high-speed DNS logging 118
                                                · and global statistics 123
                                                · and IPv6 to IPv4 mapping 106
                                                · and listeners configured for route advertisement 109
                                                · assigning to listener 122
                                                · assigning to listeners 106
                                                · configuring hardware DNS Cache 21
                                                · creating 109
                                                · creating Rapid-Response 19
                                                · creating to enable DNSSEC signing of zone transfers 57
                                                · customizing to cache DNS responses 69, 75, 82, 93, 102
                                                · customizing to handle IPv6 to IPv4 address mapping 105
                                                · enabling DNS Express 15
                                                · enabling DNS zone transfers 18, 104
                                                · enabling zone transfers 27, 33
                                                · handling non-wide IP queries 109
DNS proxy                                     · about 23, 24, 29
DNS Rapid-Response                            · and viewing statistics 20
                                                · system validation errors and warnings 19
DNS Response Cache                           · configuring 21
DNS server pools, and listeners 93
DNS servers                                   · and adding server TSIG keys 26
                                                · and creating pools 70, 92
                                                · and load balancing zone transfer requests 34
                                                · configuring to allow zone file transfers 25, 31
                                                · configuring to allow zone transfers 12
DNS servers, and zone transfers 126
DNS Services                                 · about rate-limited license statistics 131
DNS services, about IP Anycast 109
DNS statistics                               · collecting AVR statistics 121
                                                · viewing analytics in tmsh 123
                                                · viewing global 123
                                                · viewing in AVR 122
                                                · viewing per virtual server 123
DNS traffic                                    · and statistics per virtual server 123
DNS views, creating 128
DNS zone files, described 129
DNS zone proxy                                · and adding DNS nameservers to the BIG-IP system
                                                · configuration 26, 32
                                                · and DNSSEC 55
DNS zones                                     · about load balancing zone transfers to a pool of DNS
                                                · servers 29
                                                · about TSIG authentication 29
                                                · about TSIG key authentication 11, 23, 24, 30
                                                · and DNSSEC security 54, 55
                                                · and statistics 16, 103
                                                · and zone transfers 63
                                                · creating 14
                                                · creating proxy 27, 34
DNS64, configuring 105
DNSSEC                                       · and accessing SEP records for a zone 63
                                                · and DNS infrastructure illustrated 39
                                                · and dynamic signing of static zones 53, 56
                                                · and zone transfers 54, 55
                                                · configuring compliance 39
                                                · dnssec keys
                                                · and generations 64
DNSSEC keys                                   · and DNS zone proxy 55
                                                · creating for emergency rollover 40–43, 57, 59, 60
                                                · creating for key signing 42, 43, 59, 60
                                                · creating for zone signing 40, 41, 57, 59
                                                · creating key-signing keys for use with network HSM 47, 48, 51
                                                · creating zone-signing keys for use with network HSM 45, 46, 50
DNSSEC keys, about 37
DNSSEC zones                                  · and signature validation 44, 49, 53
                                                · and statistics 63
                                                · assigning keys 44, 49, 52, 61
                                                · creating 44, 49, 52, 61
DNSSEC, about 37
DS records
and SEP records 38, 81

E
effective rate limit (RPS)
about rate-limited license statistics 131
emergency rollover
and DNSSEC key-signing keys 42, 43, 59, 60
and DNSSEC zone-signing keys 40, 41, 57, 59

F
fast path DNS
about 19
file transfers, See zone file transfers.
firewall
and RPZs on the BIG-IP system 99
forward zones
and BIG-IP virtual servers as nameservers 91
and deleting nameservers 90
and DNS caches 90
and DNS caching 88
and listeners 94
and reverse zones 90
and viewing statistics 91
FPGA firmware selection
supported platforms 21

G
generations
and keys 64

H
hardware DNS Cache
configuring 21
high-speed logging
and DNS 113
and server pools 115
Hint zone, configuring using ZoneRunner 126

I
IP Anycast
about 109
and listeners 110
IPv4-only servers
and mapping to IPv6-only clients 105
passing traffic from IPv6-only clients 106
IPv6 to IPv4 mapping
and DNS profiles 105, 106
configuring listeners 106
IPv6-only clients
about mapping to IPv4-only servers 105
passing traffic to IPv4-only DNS servers 106

K
key-signing keys

key-signing keys (continued)
creating 42, 43, 59, 60
creating for use with network HSM 47, 48, 51

L
listener
applying a DNS profile 22
listeners
advertising virtual addresses 111
and IPv6 to IPv4 mapping 106
and pools of DNS servers 93
and route advertisement 111
and ZebOS 109
assigning DNS profile 122
assigning DNS profiles 106
configuring for route advertisement 110
creating to identify DNS Express traffic 15
creating to identify DNS traffic 40, 45, 50
creating to identify DNSSEC traffic 57
defined 11, 25, 31
dynamic routing protocol 109
passing traffic between IPv6-only clients and IPv4-only DNS servers 106
load balancing
zone transfer requests to a pool 29
local BIND servers, and DNS profiles 109
local zone
and DNS cache forwarding 87
local zones
adding to DNS cache for walled garden 101
and configuring DNS cache to answer DNS queries 95
and configuring DNS cache to answer DNS queries for static 87
and DNS caching 86, 88
logging
and destinations 115, 116
and pools 115
and publishers 116
DNS queries and responses 116, 117
DNS responses 117
enabling load-balancing decision logs for a wide IP 118

M
message cache
managing size 77, 84
managing size for transparent cache 72

N
named.conf
configuring using ZoneRunner 125
defined 125
nameserver cache, managing size 77, 84
nameservers
adding authoritative DNS servers 13, 62
adding DNS nameservers (clients) to BIG-IP 17, 62
adding to the BIG-IP system configuration 26, 32
adding zone transfer clients 18
and listeners 94
and modifying forward zones 90
nameservers, adding for an RPZ 99
non-wide IP queries, and custom DNS profiles 109
NOTIFY messages
  disabling TSIG verification for DNS Express zones 14
NXDOMAIN response, and RPZs 97

O
object count
  about rate-limited license statistics 131

P
pools
  and DNS servers 34, 70, 92
  for high-speed logging 115
profiles
  and disabling DNS logging 119
  creating custom DNS 69, 75, 82, 93, 102
  creating custom DNS logging 116
  creating custom DNS query and response logging 117
  creating custom DNS response logging 117
  creating custom DNS to enable zone transfers 27, 33
  creating DNS 105
  creating DNS Rapid-Response 19
  creating for DNS AVR statistics collection 121
  creating for DNS Express 15
  creating for DNS logging 118
  creating for DNS zones transfers 18, 104
  creating to enable DNSSEC signing of zone transfers 57
Protocol Validation
  configuring 21
proxy zones
  creating 27, 34
publishers
  creating for logging 116

R
Rapid-Response DNS
  and DNS profiles 19
rate rejects
  about rate-limited license statistics 131
rate-limited BIG-IP DNS license
  and viewing statistics 131
rate-limited DNS Services license
  and viewing statistics 131
remote servers
  and destinations for log messages 115, 116
  for high-speed logging 115
resolver cache
  about 73
  creating 75, 93
resolver DNS cache
  about 65
resource record cache
  managing size 77, 84
  managing size for transparent cache 72
resource records, configuring 98
response policy zone (RPZ) (continued)
  adding to a DNS cache 101
  adding to DNS caches 100
  and BIG-IP systems 97, 99
  and configuring resource records using ZoneRunner 98
  and creating a DNS Express zone 100
  configuring a zone as a distribution point 104
  creating using ZoneRunner 97
  creating with ZoneRunner 97
  staging on your network 102
reverse zones
  and forward zones 90
root nameservers, and DNS cache 95
route advertisement, and listeners 110, 111
route health injection
  about 109
  See also IP Anycast.

S
secondary DNS server
  about BIG-IP and zone transfer requests 23, 24
  about BIG-IP load balancing zone transfer requests 29
  about DNS Express 10
  and DNS Express 17
  and DNSSEC 54, 55
SEP records
  about 38, 81
  viewing 63
server pools, and listeners 93
servers
  and destinations for log messages 115, 116
  and publishers for log messages 116
  for high-speed logging 115
signature validation, of DNSSEC zones 44, 49, 53
slave DNS server
  about BIG-IP and zone transfer requests 23, 24
  about BIG-IP load balancing zone transfer requests 29
  about DNS Express 10
  and DNS Express 10, 17
  and DNSSEC 54, 55
SNMP alerts
  and cache poisoning 95
  configuring cache to generate 77, 84
static zones
  and dynamic DNSSEC signing 53, 56
statistics
  and viewing for Rapid-Response DNS traffic 20
  viewing DNS global 123
  viewing for a DNS cache 71, 76, 83, 103
  viewing for cache 70, 75, 83
  viewing for DNS cache 71, 76, 84
  viewing for DNS traffic per virtual server 123
  viewing for DNS zones 16, 103
  viewing for DNSSEC zones 63
  viewing per virtual server 123

T
tmsh, and viewing cache statistics 71, 76, 84
transparent cache
  about 67
transparent cache (continued)
creating 68
managing size 72
transparent DNS cache
about 65
trust anchors
adding to validating resolvers 81
obtaining for validating resolvers 38, 81
TSIG authentication
about 29, 30
TSIG key
adding to BIG-IP system configuration 99
TSIG key authentication
about 11, 23, 24, 29, 30
and DNS Express 17
and load balancing zone transfer requests to a pool 29
and zone transfer requests 24
TSIG key, adding to BIG-IP system configuration 13
TSIG keys
adding server TSIG 26
creating 32

U
Unsolicited Replies Threshold setting, modifying 77, 84

V
validating resolver caches
about 79
and adding DLV anchors 82
and adding trust anchors 81
and obtaining trust and DLV anchors 38, 81
creating 80
validating resolver DNS cache
about 66
views
creating for DNS in ZoneRunner 128
defined 128
virtual addresses, advertising 111

W
walled garden
and adding local zone to DNS cache 101
and RPZs on the BIG-IP system 97
wide IPs
enabling load-balancing decision logging 118

Z
ZebOS dynamic routing protocol
and listeners 110
enabling 109
verifying route advertisement 111
zone file transfers, and configuring DNS servers 25, 31
zone transfer requests
and BIG-IP as zone proxy 24
and DNS Express 17
and DNS zones 18
load balancing to a pool 29
zone transfer requests (continued)
load balancing using TSIG authentication 30
zone transfers
about configuring for RPZs 103
and configuring DNS servers 12
and DNSSEC 54, 55
zone transfers, and BIG-IP DNS 126
zone-signing keys
creating 40, 41, 57, 59
creating for use with network HSM 45, 46, 50
ZoneRunner
about 125
and configuring a hint zone 126
and configuring a zone 125
and configuring named 125
and configuring resource records for an RPZ 98
and creating DNS views 128
creating an RPZ 97
creating RPZs 97
zones
and zone transfers 63
configuring hint 126
configuring using ZoneRunner 125
creating 14
protecting from DDoS attacks 14
zones creating DNSSEC 44, 49, 52, 61
See also DNSSEC zones.
zones transfers
and RPZs 104