



Deploying the BIG-IP System v11 with DNS Servers

What's inside:

- 2 Prerequisites and configuration notes
- 2 Configuration example
- 3 Preparation Worksheet
- 4 Configuring the BIG-IP iApp for DNS Servers
- 6 Next steps

Welcome to the F5 deployment guide for DNS servers. This document contains guidance on configuring the BIG-IP system version 11 for intelligent traffic management for DNS servers, resulting in a secure, fast, and available deployment.

BIG-IP version 11.0 introduces iApp™ Application templates, an extremely easy way to configure the BIG-IP system for your DNS servers.

Why F5?

The BIG-IP system provides more sophisticated ways to receive and respond to DNS requests than standard DNS load balancing. LTM uses advanced monitors to ensure traffic is only sent to available DNS servers that are responding with the correct records, and includes built-in protection against DNS denial-of-service attacks.

To provide feedback on this deployment guide or other F5 solution documents, contact us at solutionsfeedback@f5.com.

Products and versions tested

Product	Version
BIG-IP LTM	v11

Important: Make sure you are using the most recent version of this deployment guide, available at <http://www.f5.com/pdf/deployment-guides/dns-iapp-dg.pdf>.

What is F5 iApp™?

New to BIG-IP version 11, F5 iApp is a powerful new set of features in the BIG-IP system that provides a new way to architect application delivery in the data center, and it includes a holistic, application-centric view of how applications are managed and delivered inside, outside, and beyond the data center. The iApp template for DNS servers acts as the single-point interface for building, managing, and monitoring these servers.

For more information on iApp, see the White Paper *F5 iApp: Moving Application Delivery Beyond the Network*: <http://www.f5.com/pdf/white-papers/f5-iapp-wp.pdf>.

Document Version

1.0

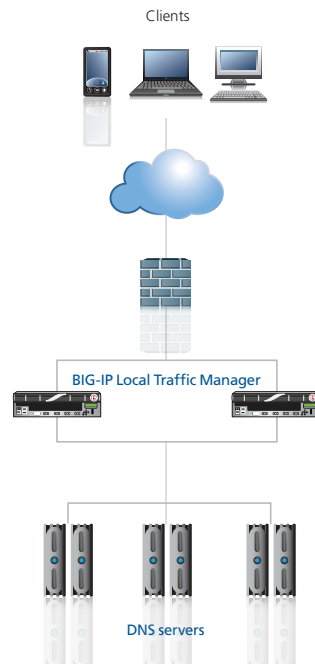
Prerequisites and configuration notes

The following are general prerequisites and configuration notes for this guide:

- For this deployment guide, the BIG-IP LTM system **must** be running version 11.0 or later. If you are using a previous version of the BIG-IP LTM system, see the Deployment Guide index on F5.com. The configuration described in this guide does not apply to previous versions.
- This deployment guide provides guidance for using the iApp for DNS servers found in version 11.0 and later. For advanced users extremely familiar with the BIG-IP, there is a manual configuration table at the end of this guide. However, we strongly recommend using the iApp template.
- This guide does not contain information on configuring DNS servers. See your DNS server documentation for configuring these servers.

Configuration example

In this Deployment Guide, the BIG-IP system is optimally configured to optimize and direct traffic to DNS servers. The following diagram shows a logical configuration example with a redundant pair of BIG-IP LTM devices, in front of a group of DNS servers.



Preparation Worksheet

In order to use the iApp for DNS servers, you need to gather some information, such as server IP addresses and domain information. Use the following worksheet to gather the information you will need while running the template. The worksheet does not contain every question in the template, but rather includes the information that is helpful to have in advance. More information on specific template questions can be found on the individual pages.

You might find it useful to print this table and then enter the information.

➡ **Note:** *Although we show space for 10 pool members, you may have more or fewer members in each pool.*

IP Addresses/FQDN	Pool Members	Sync/Failover Groups*	Health Monitor	WAN or LAN clients
IP address you will use for the LTM virtual server:	DNS server IP addresses: 1: 2: 3: 4: 5: 6: 7: 8: 9: 10: Port used by the server:	If using the Advanced feature of Sync/Failover Groups, you must already have a Device Group and a Traffic Group Device Group name: Traffic Group name:	What record type to you want to use to test the DNS Servers: A NS PTR SOA CNAME Host name to send to the DNS server: IP address you expect to be returned from DNS server to be considered healthy:	Most clients connecting through BIG-IP to the HTTP server are coming over a: LAN WAN

Configuring the BIG-IP iApp for DNS Servers

Use the following guidance to help you configure the BIG-IP system for DNS Servers using the BIG-IP iApp template.

Getting Started with the iApp for DNS Servers

To begin the DNS iApp Template, use the following procedure.

1. Log on to the BIG-IP system.
2. On the Main tab, expand **iApp**, and then click **Application Services**.
3. Click **Create**. The Template Selection page opens.
4. In the **Name** box, type a name. In our example, we use **DNS-servers_**.
5. From the **Template** list, select **f5.dns**.
The DNS template opens.

Advanced options

If you select Advanced from the Template Selection list, you see Sync and Failover options for the application. This feature, new to v11, is a part of the Device Management configuration. This functionality extends the existing High Availability infrastructure and allows for clustering, granular control of configuration synchronization and granular control of failover. For more information on Device Management, see the Online Help or product documentation.

1. **Configure Sync/Failover?**
If you want to configure the Application for Sync or failover groups, select **Yes** from the list.
 - a. **Device Group**
If you select Yes from the question above, the Device Group and Traffic Group options appear. If necessary, uncheck the Device Group box and then select the appropriate Device Group from the list.
 - b. **Traffic Group**
If necessary, uncheck the Traffic Group box and then select the appropriate Traffic Group from the list.

Virtual Server Questions

The next section of the template asks questions about the BIG-IP virtual server. A virtual server is a traffic-management object on the BIG-IP system that is represented by an IP address and a service. Clients can send traffic to a virtual server, which then directs the traffic according to your configuration instructions.

1. **IP address for the virtual server**
This is the address clients use to access the DNS servers (or a FQDN will resolve to this address). You need an available IP address to use here.
2. **Routes or secure network address translation**
If the DNS servers do not have a route back for clients through the BIG-IP, i.e. if they do not use the BIG-IP as the default gateway, the BIG-IP uses Secure Network Address Translation (SNAT) Automap (exception in #3) to translate the client's source address to an address configured on the BIG-IP. The servers then use this new source address as the destination address when responding to traffic originating through the BIG-IP.

If you indicate the servers do have a route back to the clients through the BIG-IP, the BIG-IP does not translate the client's source address; in this case, you must make sure the BIG-IP is configured as the gateway to the client networks (usually the default gateway) on the servers.

We recommend choosing **No** from the list because it is secure and does not require you to configure routing manually.

If you are configuring your BIG-IP LTM in a "one-armed" configuration with your servers -- where the BIG-IP virtual server(s) and the servers have IP addresses on the same subnet -- you must choose **No**.

3. **More than 64,000 simultaneous connections**

If you do not expect more than 64,000 simultaneous connections, leave this answer set to **No** and continue with the next section.

If you have a large deployment and expect more than 64,000 connections at one time, the iApp creates a SNAT Pool instead of using SNAT Automap. With a SNAT Pool, you need one IP address for each 64,000 connections you expect. Select **Yes** from the list. A new row appears with an IP address field. In the **Address** box, type an IP address and then click **Add**. Repeat for any additional IP addresses.

Server Pool, Load Balancing, and Service Monitor questions

In this section, you add the DNS servers, and configure the health monitor and pool.

1. **New Pool**

Choose **Create New Pool** unless you have already made a pool on the LTM for the DNS devices.

2. **Load balancing method**

While you can choose any of the load balancing methods from the list, we recommend the default, **Least Connections (member)**.

3. **Address/Port**

Type the IP Address and Port for each DNS server. You can optionally add a Connection Limit. Click **Add** to add additional servers to the pool.

Protocol Optimization Questions

In this section, you configure protocol optimizations.

1. **WAN or LAN**

Specify whether most clients are connecting over a WAN or LAN.

Health monitor questions

1. **Record type**

This question asks what DNS record type you want to use to test the DNS servers. The choices are A, NS, PTR, SOA, and CNAME. For more information on DNS record types, see your DNS documentation.

2. **Host name**

Type the host name you want to send the DNS server for this health monitor. The BIG-IP system sends a request to the DNS servers for this host name to determine server availability.

3. **IP address**

Type the IP address you expect to receive from the DNS servers as a response to the host name request above. The DNS server will be considered available if this IP address is returned from the host name request.

Finished

Review the answers to your questions. When you are satisfied, click the **Finished** button. The BIG-IP system creates the relevant objects for the DNS servers.

Next steps

After completing the iApp Template, the BIG-IP Application Services page opens for the DNS service you just created. To see the list of all the configuration objects created to support the DNS servers, on the Menu bar, click **Components**. The complete list of all related objects opens. You can click individual objects to see the settings.

Once the objects have been created, you are ready to use the new deployment.

Modifying DNS settings to use the BIG-IP virtual server address

Before sending traffic to the BIG-IP system, your DNS administrator may need to modify any DNS entries for this DNS server implementation to point to the BIG-IP system's virtual server address.

Modifying the iApp configuration

The iApp application service you just created can be quickly and easily modified if you find it necessary to make changes to the configuration. The Strict Updates feature of the iApp prevents users from manually modifying the iApp configuration (Strict Updates can be turned off, but use extreme caution). iApp allows you to re-enter the template, make changes, and then update the template. The modifications are automatically made to any of the associated objects.

To modify the configuration

1. On the Main tab, expand **iApp** and then click **Application Services**.
2. Click the name of your DNS server Application Service from the list.
3. On the Menu bar, click **Reconfigure**.
4. Make the necessary modifications to the template.
5. Click the **Finished** button.

Viewing statistics

You can easily view a number of different statistics on the BIG-IP system related to the configuration objects created by the iApp template.

To view object-level statics

1. On the Main tab, expand **Overview**, and then click **Statistics**.
2. From the **Statistics Type** menu, you can select **Virtual Servers** to see statistics related to the virtual servers.
3. You can also choose **Pools** or **Nodes** to get a closer look at the traffic.
4. To see Networking statistics in a graphical format, click **Dashboard**.

For more information on viewing statistics on the BIG-IP system, see the online help or product documentation.

Appendix: Manual configuration table

We strongly recommend using the iApp template to configure the BIG-IP system for DNS load balancing. Advanced users extremely familiar with the BIG-IP system can use the following table to manually configure the BIG-IP system.

One of the strengths of this deployment is the health monitor. The iApp template uses a UDP monitor and creates a hex string for Send String in the monitor, which represents the DNS query. It also creates a Receive String as a hex string representing the IP address part of DNS response. Because of the complexity in manually recreating these monitors, we do not provide manual guidance, but recommend you run the DNS iApp to create the monitors. The rest of the configuration does not have to use real values, only the monitor section. You will then associate the monitor created by the iApp with the manual configuration you perform below.

The following table contains a list of BIG-IP LTM configuration objects along with any non-default settings you should configure as a part of this deployment. Unless otherwise specified, settings not mentioned in the table can be configured as applicable for your configuration. For specific instructions on configuring individual objects, see the online help or product manuals.

BIG-IP LTM Object	Non-default settings/Notes	
Health Monitor	Use the iApp to create the health monitor as described in the 2nd paragraph of the introduction above.	
Pool (Main tab-->Local Traffic -->Pools)	Name	Type a unique name
	Health Monitor	Select the monitor created by the template.
	Slow Ramp Time¹	300
	Load Balancing Method	Choose a load balancing method. We use the default Round Robin
	Address	Type the IP Address of the DNS nodes
	Service Port	53 (click Add to repeat Address and Service Port for all nodes)
Profiles (Main tab-->Local Traffic -->Profiles)	TCP WAN (Profiles-->Protocol)	Name: Type a unique name Parent Profile: tcp-wan-optimized
	TCP LAN (Profiles-->Protocol)	Name: Type a unique name Parent Profile: tcp-lan-optimized
	UDP (Profiles-->Protocol)	Name: Type a unique name
		Parent Profile: UDP
		Datagram LB: Enabled
	Virtual Servers (Main tab-->Local Traffic -->Virtual Servers)	TCP
Name		Type a unique name
Address		Type the IP Address for the virtual server
Service Port		53
Protocol Profile (client)¹		Select the WAN optimized TCP profile you created above
Protocol Profile (server)¹		Select the LAN optimized TCP profile you created above
SNAT Pool²		Automap (optional; see footnote ²)
Default Pool		Select the pool you created above
UDP		
Name		Type a unique name
Address		Type the IP Address for the virtual server
Service Port		53
Protocol		Select UDP from the list.
Protocol Profile (client)¹		Select the WAN optimized TCP profile you created above
SNAT Pool²		Automap (optional; see footnote ²)
Default Pool	Select the pool you created above	

¹ You must select **Advanced** from the **Configuration** list for these options to appear

² If want to use SNAT, and you have a large deployment expecting more than 64,000 simultaneous connections, you must configure a SNAT Pool with an IP address for each 64,000 simultaneous connections you expect. See the BIG-IP documentation on configuring SNAT Pools.

Document Revision History

Version	Description
1.0	New Version

F5 Networks, Inc. 401 Elliott Avenue West, Seattle, WA 98119 888-882-4447 www.f5.com

F5 Networks, Inc.
Corporate Headquarters
info@f5.com

F5 Networks
Asia-Pacific
apacinfo@f5.com

F5 Networks Ltd.
Europe/Middle-East/Africa
emeainfo@f5.com

F5 Networks
Japan K.K.
f5j-info@f5.com

