Deploying the BIG-IP System for DNS Traffic Management

Welcome to the F5 deployment guide for DNS traffic management. This guide provides step-by-step procedures for configuring the BIG-IP system version 11.4 and later for load balancing and intelligent traffic management for DNS servers. BIG-IP version 11.0 introduced iApp™ Application templates, an extremely easy way to accurately configure the BIG-IP system for your DNS servers.

Products and Versions tested

Product	Versions
BIG-IP LTM	11.4, 11.4.1, 11.5, 11.5.1, 11.6
DNS	Not applicable
DNS iApp template	System iApp that ships with v11.4 and later
Deployment Guide version	1.4 (see *Document Revision History on page 19)*

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

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

Contents

Why F5?

The BIG-IP system provides more sophisticated ways to receive and respond to DNS requests than standard DNS load balancing. The BIG-IP Local Traffic Manager (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.

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 acts as the single-point interface for building, managing, and monitoring your DNS deployment.

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*.

Prerequisites and configuration notes

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

- For this deployment guide, the BIG-IP system ***must*** be running version 11.4 or later. If you are using a previous version of the BIG-IP system, see the deployment guide index on F5.com. The configuration in this guide does not apply to previous versions.
- If you upgraded your BIG-IP system from a previous v11 version, and have an existing Application Service that used the f5.dns iApp template, see *Upgrading an Application Service from previous version of the iApp template on page 14*.
- This document provides guidance for using the iApp for DNS found in version 11.4 and later. For users familiar with the BIG-IP system, there is a manual configuration table at the end of this guide. However, we 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 scenarios

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

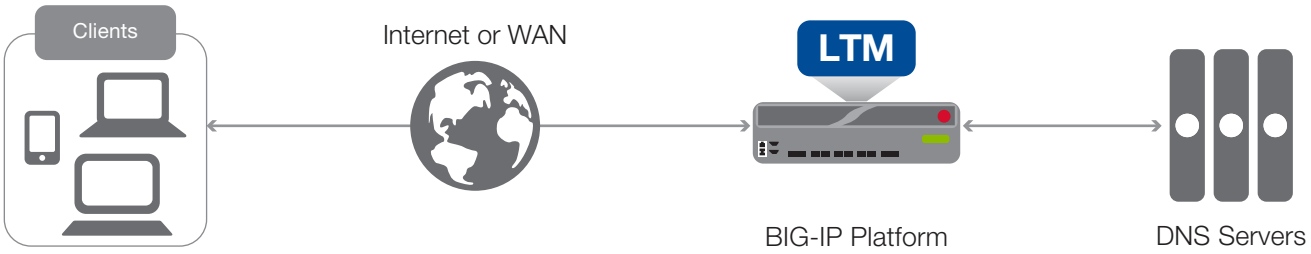

Figure 1: *Logical configuration example*

Using this guide

This guide is intended to help users deploy web-based applications using the BIG-IP system. This deployment guide contains guidance on two ways to configure the BIG-IP system: using the iApp template, and manually configuring the BIG-IP system.

Using this guide to configure the App template

We recommend using the iApp template to configure the BIG-IP system for your DNS implementation. The majority of this guide describes the iApp template and the different options the template provides for configuring the system for DNS servers.

The iApp template configuration portion of this guide walks you through the entire iApp, giving detailed information not found in the iApp or inline help. The questions in the iApp template itself are all in a table and at the same level. In this guide, we have grouped related questions and answers in a series of lists. Questions are part of an ordered list and are underlined and in italics or bold italics. Options or answers are part of a bulleted list, and in bold. Questions with dependencies on other questions are shown nested under the top level question, as shown in the following example:

1. ***Top-level question found in the iApp template***
   - *Select an object you already created from the list* (such as a profile or pool; not present on all questions. Shown in bold italic)
   - **Choice #1** (in a drop-down list)
   - **Choice #2** (in the list)
     a. *Second level question dependent on selecting choice #2*
        - **Sub choice #1**
        - **Sub choice #2**
          i). *Third level question dependent on sub choice #2*
              - **Sub-sub choice**
              - **Sub-sub #2**
                1). *Fourth level question (rare)*

Manually configuring the BIG-IP system

Users already familiar with the BIG-IP system can use the manual configuration tables to configure the BIG-IP system for the DNS implementation. These configuration tables only show the configuration objects and any non-default settings recommended by F5, and do not contain procedures on specifically how to configure those options in the Configuration utility. See *Appendix: Manual configuration table on page 15.*

Preparing to use the iApp

In order to use the iApp for DNS servers, it is helpful to have some information, such as server IP addresses and domain information before you begin. Use the following table for information you may need to complete the template. The table 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.

<table>
<tr><th colspan="3">BIG-IP LTM Preparation table</th></tr>
<tr><td>Basic/Advanced mode</td><td colspan="2">In the iApp, you can configure your DNS implementation with F5 recommended settings (Basic mode) which are a result of extensive testing and tuning with DNS servers. Advanced mode gives you the to configure the BIG-IP system on a much more granular level, configuring specific options, or even using your own pre-built profiles or iRules. Basic and Advanced "configuration mode" is independent from the Basic/Advanced list at the very top of the template which only toggles the Device and Traffic Group options (see page 6)</td></tr>
<tr><td rowspan="2">Network</td><td>Where are BIG-IP virtual servers in relation to the servers</td><td>Expected number of concurrent connections per server</td></tr>
<tr><td>Same subnet | Different subnet

If they are on different subnets, you need to know if the servers have a route through the BIG-IP system. If there is not a route, you need to know the number of concurrent connections.</td><td>More than 64k concurrent | Fewer than 64k concurrent

If more than 64k per server, you need an available IP address for each 64k connections you expect for the SNAT Pool</td></tr>
<tr><td rowspan="2">Virtual Server and Pools</td><td>Virtual Server</td><td>DNS server pool</td></tr>
<tr><td>The Virtual server is the address clients use to access the servers.

IP address for the virtual server:

Associated service port (default for DNS is 53):</td><td>The load balancing pool is the LTM object that contains the servers.

IP addresses of the servers: 1: 3:
2: 5:
4: 7:
6: 9:
8:</td></tr>
<tr><td>Profiles</td><td colspan="2">For each of the following profiles, the iApp will create a profile using the F5 recommended settings (or you can choose ‘do not use’ many of these profiles). While we recommend using the profiles created by the iApp, you have the option of creating your own custom profile outside the iApp and selecting it from the list. The iApp gives the option of selecting our the following profiles (some only in Advanced mode). Any profiles must be present on the system before you can select them in the iApp

TCP LAN | TCP WAN | UDP</td></tr>
<tr><td>iRules</td><td colspan="2">In Advanced mode, you have the option of attaching iRules you create to the virtual server created by the iApp. For more information on iRules, see https://devcentral.f5.com/irules Any iRules you want to attach must be present on the system at the time you are running the iApp.</td></tr>
</table>

Configuring the BIG-IP iApp for DNS servers

Use the following guidance to help 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-iapp_.**
5. From the **Template** list, select **f5.dns**. The DNS template opens.

Advanced options

If you select **Advanced** from the **Template Selection** list at the top of the page, you see Device and Traffic Group 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. To use the Device and Traffic Group features, you must have already configured Device and Traffic Groups before running the iApp. For more information on Device Management, see the product documentation.

1. ***Device Group***
   To select a specific Device Group, clear the **Device Group** check box and then select the appropriate Device Group from the list.
2. ***Traffic Group***
   To select a specific Traffic Group, clear the **Traffic Group** check box and then select the appropriate Traffic Group from the list.

Template Options

This section contains general questions about the way you configure the iApp template.

1. ***Do you want to see inline help?***
   Choose whether you want to see informational and help messages inline throughout the template, or if you would rather hide this inline help. If you are unsure, we recommend having the iApp display the inline help.
   Important and critical notes are always shown, no matter which selection you make.
   - **Yes, show inline help text**
     Select this option to see all available inline help text.
   - **No, do not show inline help text**
     If you are familiar with this iApp template, or with the BIG-IP system in general, select this option to hide the inline help text.

2. ***Which configuration mode do you want to use?***
   Select whether you want to use F5 recommended settings, or have more granular, advanced options presented.
   - **Basic - Use F5's recommended settings**
     In basic configuration mode, options like load balancing method and parent profiles are all set automatically. The F5 recommended settings come as a result of extensive testing with web applications, so if you are unsure, choose Basic.
   - **Advanced - Configure advanced options**
     In advanced configuration mode, you have more control over individual settings and objects, such as server-side optimizations and advanced options like Slow Ramp Time and Priority Group Activation. You can also choose to attach iRules you have previously created to the application service. The Advanced option provides more flexibility for experienced users.

     Advanced options in the template are marked with the Advanced icon: Advanced. If you are using Basic/F5 recommended settings, you can skip the questions with this icon.

Network

This section contains questions about your networking configuration. This whole section only appears if you selected Advanced mode.

1. ***What type of network connects clients to the BIG-IP system?*** Advanced
   Choose the type of network that connects your clients to the BIG-IP system. The BIG-IP system uses this information to determine the appropriate TCP optimizations.

   - **Local area network (LAN)**
     Select this option if most clients are connecting to the BIG-IP system on a LAN. This field is used to determine the appropriate TCP profile which is optimized for LAN clients. In this case, the iApp creates a TCP profile using the *tcp-lan-optimized* parent with no additional modifications.
   - **Wide area network**
     Select this option if most clients are connecting to the BIG-IP system over a WAN. This field is used to determine the appropriate TCP profile which is optimized for WAN clients. In this case, the iApp creates a TCP profile using the *tcp-wan-optimized* parent with no additional modifications.

2. ***Which VLANs transport client traffic?*** Advanced
   The BIG-IP system allows you to restrict client traffic to specific BIG-IP VLANs, which can provide an additional layer of security, as only traffic from the VLANs you select are allowed to the servers. By default, all VLANs configured on the system are enabled. Select which of your BIG-IP VLANs are transporting client traffic. If you want the BIG-IP system to only accept client traffic from specific VLANs, from the **Selected** list, select the appropriate VLAN(s) from which you do not want the system to accept traffic, and then click the Remove (**>>**) button to move the VLAN to the Option box.

   Note

   If you choose to allow traffic from certain VLANs, when additional VLANs are added to the BIG-IP system at a later time, this iApp configuration will deny traffic from these VLANs by default. To accept traffic from these VLANs, you must re-enter the template and add the VLAN(s).

3. ***What type of network connects servers to the BIG-IP system?*** Advanced
   Choose the type of network that connects your servers to the BIG-IP system. Similar to the question about clients connecting to the BIG-IP system, the system uses this information to determine the appropriate TCP optimizations.

   - **Local area network (LAN)**
     Select this option if the servers connect to the BIG-IP system on a LAN. This field is used to determine the appropriate TCP profile. In this case, the iApp creates a TCP profile using the *tcp-lan-optimized* parent with no additional modifications.
   - **Wide area network**
     Select this option if the servers connect to the BIG-IP system over a WAN. This field is used to determine the appropriate TCP profile. In this case, the iApp creates a TCP profile using the *tcp-wan-optimized* parent with no additional modifications.

4. ***Where will your BIG-IP virtual servers be in relation to the DNS servers?*** Advanced
   Select whether your BIG-IP virtual servers are on the same subnet as your DNS servers, or on different subnets. This setting is used to determine the *SNAT* (secure NAT) and routing configuration.

   - **BIG-IP virtual server IP and web servers are on the same subnet**
     If the BIG-IP virtual servers and DNS servers are on the same subnet, SNAT is configured on the BIG-IP virtual server and you must specify the number of concurrent connections.

     a. *How many connections per server do you expect?*
        Select whether you expect more or fewer than 64,000 concurrent connections to each server. This answer is used to determine what type of SNAT that system uses. A SNAT is an object that maps the source client IP address in a request to a translation address defined on the BIG-IP device. The system configures SNAT Auto Map (fewer than 64,000) or a SNAT pool (more than 64,000).

- **Fewer than 64,000 concurrent connections**
  Select this option if you expect fewer than 64,000 concurrent connections per web server. With this option, the system applies SNAT Auto Map, doesn't require any additional IP addresses, as an existing self IP address is used for translation. Continue with the next section.
- **More than 64,000 concurrent connections**
  Select this option if you have a very large deployment and expect more than 64,000 connections at one time. The iApp creates a SNAT Pool, for which you need one IP address for each 64,000 connections you expect.

  i). Create a new SNAT pool or use an existing one?
  If you have already created a SNAT pool on the BIG-IP system, you can select it from the list. Otherwise, the system creates a new SNAT pool with the addresses you specify.

  - **Create a new SNAT pool**
    Select this option (the default) to enable the system to create a new SNAT pool. You must specify the appropriate number of IP addresses in the next question.

    1). Which IP addresses do you want to use for the SNAT pool?
    Specify one otherwise unused IP address for every 64,000 concurrent connections you expect, or fraction thereof. Click **Add** for additional rows. Do not use any self IP addresses on the BIG-IP system.

  - **Select a SNAT poo**/
    Select the SNAT pool you created for this deployment from the list.

    Important

    If you choose more than 64,000 connections, but do not specify enough SNAT pool address(es), after the maximum connection limit of 64,000 concurrent connections per DNS server is reached, new requests fail.

- **BIG-IP virtual servers and DNS servers are on different subnets**
  If the BIG-IP virtual servers and servers are on different subnets, the following question appears.

  a. How have you configured routing on your DNS servers?
  If you chose different subnets, this question appears asking whether the web servers use this BIG-IP system's self IP address as their default gateway. Select the appropriate answer.

  - **DNS servers have a route to clients through the BIG-IP system**
    Choose this option if the servers use the BIG-IP system as their default gateway. In this case, no configuration is needed to support your environment to ensure correct server response handling. Continue with the next section.
  - **DNS servers do not have a route to clients through the BIG-IP**
    If the DNS servers do not use the BIG-IP system as their default gateway, *SNAT* is configured on the BIG-IP virtual server and you must select the expected number of concurrent connections in the next question.

    i). How many connections per server do you expect?
    Select whether you expect more or fewer than 64,000 concurrent connections to each server. This answer is used to determine what type of SNAT that system uses. A SNAT is an object that maps the source client IP address in a request to a translation address defined on the BIG-IP device. The system configures SNAT Auto Map (fewer than 64,000) or a SNAT pool (more than 64,000).

    - **Fewer than 64,000 concurrent connections**
      Select this option if you expect fewer than 64,000 concurrent connections per server. With this option, the system applies SNAT Auto Map, doesn't require any additional IP addresses, as an existing self IP address is used for translation. Continue with the next section.
    - **More than 64,000 concurrent connections**
      Select this option if you have a very large deployment and expect more than 64,000 connections at one time. The iApp creates a SNAT Pool, for which you need one IP address for each 64,000 connections you expect.

1). *Create a new SNAT pool or use an existing one?*
If you have already created a SNAT pool on the BIG-IP system, you can select it from the list. Otherwise, the system creates a new SNAT pool with the addresses you specify.

* **Create a new SNAT pool**
Select this option (the default) to enable the system to create a new SNAT pool. You must specify the appropriate number of IP addresses in the next question.

a). *Which IP addresses do you want to use for the SNAT pool?*
Specify one otherwise unused IP address for every 64,000 concurrent connections you expect, or fraction thereof. Click **Add** for additional rows. Do not use any self IP addresses on the BIG-IP system.

* **Select a SNAT pool**
Select the SNAT pool you created for this deployment from the list.

Important

If you choose more than 64,000 connections, but do not specify enough SNAT pool address(es), after the maximum connection limit of 64,000 concurrent connections per server is reached, new requests fail.

High Availability

This section gathers information about your DNS deployment that will be used in the BIG-IP *virtual server* and *load balancing pool*.

1. ***What IP address do you want to use for the virtual server?***
Type the IP address you want to use for the BIG-IP virtual server. This is the address clients use (or a DNS entry resolves to this address) to access the DNS deployment via the BIG-IP system.

2. ***What is the associated service port?***
Type the port number you want to use for the BIG-IP virtual server. For DNS deployments, this is **53**.

3. ***Do you want to create a new pool or use an existing one?***
A *load balancing pool* is a logical set of servers, grouped together to receive and process traffic. When clients attempt to access the servers via the BIG-IP virtual server, the BIG-IP system distributes requests to any of the servers that are members of that pool.

- *Select an existing pool*
If you have already created a pool for your DNS servers, you can select it from the list.
If you do select an existing pool, all of the rest of the questions in this section disappear.

- **Create a new pool**
Leave this default option to create a new load balancing pool and configure specific options.

a. *Which load balancing method do you want to use?* Advanced
Specify the load balancing method you want to use for this DNS server pool. For DNS, we recommend the default, **Least Connections (member)**.

b. *Do you want the BIG-IP system to queue TCP requests?* Advanced
Select whether you want the BIG-IP system to queue TCP requests. TCP request queuing provides the ability to queue connection requests that exceed the capacity of connections for a pool, as determined by the connection limit. Consequently, instead of dropping connection requests that exceed the capacity of a pool, TCP request queuing enables those connection requests to reside within a queue according to defined conditions until capacity becomes available. For more information on TCP Request Queuing, see the *Preventing TCP Connection Requests From Being Dropped* chapter in the ***BIG-IP Local Traffic Manager: Implementations*** guide, available on AskF5.

Important

TCP Request Queuing is an advanced feature and should be used only if you understand how it will affect your deployment, including application behavior and BIG-IP performance.
If you enable TCP Request Queuing, you must have a Connection Limit set on at least one of the nodes when configuring the Address/Port.

- **Do not enable TCP request queuing**
  Select this option if you do not want the BIG-IP system to queue TCP requests.
- **Enable TCP request queuing**
  Select this option if you want to enable TCP request queuing on the BIG-IP system.
  i). *What is the maximum number of TCP requests for the queue?*
  Type the maximum number of requests you want to queue. We do ***not*** recommend using 0, which means unlimited and is only constrained by available memory.
  ii). *How many milliseconds should requests remain in the queue?*
  Type a number of milliseconds for the TCP request timeout value.

c. *Use a Slow Ramp time for newly added servers?* **Advanced**
With Slow Ramp, the BIG-IP system gradually adds connections to a newly-enabled or newly-added server over a time period you specify, rather than sending a full proportion of the traffic immediately. Slow Ramp is essential when using load balancing methods like Least Connections, as the system would otherwise send all new connections to a new server immediately, potentially overwhelming that server.

Select whether you want to use a Slow Ramp time.

- **Use Slow Ramp**
  Select this option for the system to implement Slow Ramp time for this pool.
  i). *How many seconds should Slow Ramp time last?*
  Specify a duration in seconds for Slow Ramp. The time period you select for Slow Ramp is highly dependent on the speed of your server hardware and the behavior of your services. The default setting of 300 seconds (5 minutes) is very conservative in most cases.
- **Do not use Slow Ramp**
  Select this option if you do not want to use Slow Ramp. If you select this option, we recommend you do not use the Least Connections load balancing method.

d. *Do you want give priority to specific groups of servers?* **Advanced**
Select whether you want to use Priority Group Activation. Priority Group Activation allows you to segment your servers into priority groups. With Priority Group Activation, the BIG-IP system load balances traffic according to the priority number you assign to the pool members. A higher number indicates higher priority. Traffic is only sent to the servers with the highest priority, unless the number of available servers in that priority group falls below the value you specify as the minimum. The BIG-IP system then sends traffic to the group of servers with the next highest priority, and so on. See the BIG-IP documentation for more details.

- **Do not use Priority Group Activation**
  Select this option if you do not want to enable Priority Group Activation.
- **Use Priority Group Activation**
  Select this option if you want to enable Priority Group Activation.
  You must add a priority to each server in the Priority box described in #e.
  i). *What is the minimum number of active members in a group?*
  Specify the minimum number of servers that must be active to continue sending traffic to the priority group. If the number of active servers falls below this minimum, traffic will be sent to the group of servers with the next highest priority group number.

e. *Which DNS servers are a part of this pool?*
Specify the IP address(es) of your DNS servers. If you have existing nodes on this BIG-IP system, you can select them from the list, otherwise type the addresses. You can optionally add a Connection Limit. If you enabled Priority Group Activation, you must also specify a Priority for each device. Click **Add** to include additional servers.

Application Health

In this section, you answer questions about how you want to implement application health monitoring on the BIG-IP system.

1. ***Create a new health monitor or use an existing one?***
Application health monitors are used to verify the DNS servers are available and functioning.

   Unless you have requirements for configuring other options not in the following list of questions, we recommend allowing the iApp to create a new monitor. Creating a custom health monitor is not a part of this template; see **Local Traffic** >> **Monitors**. To select any new monitors you create, you need to restart or reconfigure this template.

   - *Select the monitor you created from the list*
   If you manually created the health monitor for your DNS servers, select it from the list. Continue with the next section.
   - **Create a new health monitor**
   If you want the iApp to create a new DNS monitor, continue with the following.

      a. *How many seconds between health checks?*
      Specify how long the system should wait between each health check. This is used as the Interval setting for the monitor. We recommend the default of 30 seconds.

      b. *What record type do you want to use to test these DNS servers?*
      Specify whether you want to use an A or AAAA DNS record type to test the DNS servers. For more information on DNS record types, see your DNS documentation.

      c. *What fully qualified hostname do you want to send to the DNS server for this health monitor?*
      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.

      d. *What IP address do you expect back from a healthy DNS server?*
      Specify the IP address you expect to be returned from the DNS servers for host name you entered in the previous question. The server is considered healthy if the IP address you enter here is returned. If you leave this field blank, the BIG-IP system marks the server up if the DNS response code is **no-error**.

Client Optimization

In this section, you answer questions about how you want the BIG-IP system to optimize the client-side delivery of your DNS traffic.

1. ***How do you want to optimize client-side connections?*** Advanced
The client-side TCP profile optimizes the communication between the BIG-IP system and the client by controlling the behavior of the traffic which results in higher transfer rates, improved connection reliability and increased bandwidth efficiency.

   Unless you have requirements for configuring specific TCP optimization settings, we recommend allowing the iApp to create a new profile. Creating a custom profile is not a part of this template; see **Local Traffic** >> **Profiles** : **Protocol : TCP** to create a TCP profile. To select any new profiles you create, you need to restart or reconfigure this template.

   - *Select the TCP profile you created from the list*
   If you created a custom TCP profile for the DNS servers, select it from the list.
   - **New profile based on tcp-wan-optimized (recommended)**
   Select this option to have the system create a new TCP profile optimized for WAN clients. The system creates a TCP profile using the tcp-wan-optimized parent profile.

Server Optimization

In this section, you answer questions about how you want the BIG-IP system to optimize the server-side delivery of your DNS traffic.

1. ***How do you want to optimize server-side connections?*** Advanced
   The server-side TCP profile optimizes the communication between the BIG-IP system and the server by controlling the behavior of the traffic which results in higher transfer rates, improved connection reliability and increased bandwidth efficiency.

   Unless you have requirements for configuring specific TCP optimization settings, we recommend allowing the iApp to create a new profile. Creating a custom profile is not a part of this template; see **Local Traffic** >> **Profiles** : **Protocol : TCP** to create a TCP profile. To select any new profiles you create, you need to restart or reconfigure this template.

   - *Select the TCP profile you created from the list*
     If you created a custom TCP profile for the DNS servers, select it from the list.
   - **New profile based on tcp-lan-optimized (recommended)**
     Select this option to have the system create a new TCP profile optimized for LAN clients. The system creates a TCP profile using the tcp-lan-optimized parent profile.

iRules

In this section, you can add custom iRules to the DNS deployment. This entire section is available only if you selected Advanced mode. Because the iApp template creates two virtual servers, one for TCP traffic and one for UDP traffic, there are separate questions for attaching iRules to the individual virtual server.

iRules are a scripting language that allows an administrator to instruct the system to intercept, inspect, transform, direct and track inbound or outbound application traffic. An iRule contains the set of instructions the system uses to process data flowing through it, either in the header or payload of a packet.

Warning

While iRules can provide additional functionality not present in the iApp, iRules are an advanced feature and should be used only if you understand how each iRule will affect your deployment, including application behavior and BIG-IP system performance.

1. ***Do you want to add any custom iRules to the TCP virtual server?*** Advanced
   Select if have preexisting iRules you want to add to the TCP portion of your DNS implementation.

   If you have iRules you want to attach to the TCP virtual server the iApp creates for your DNS servers, from the **Options** box, click the name of the applicable iRule(s) and then click the Add (**<<**) button to move them to the **Selected** box.

2. ***Do you want to add any custom iRules to the UDP virtual server?*** Advanced
   Select if have preexisting iRules you want to add to the UDP portion of your DNS implementation.

   If you have iRules you want to attach to the UDP virtual server the iApp creates for your DNS servers, from the **Options** box, click the name of the applicable iRule(s) and then click the Add (**<<**) button to move them to the **Selected** box.

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 implementation.

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 DNS, 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 the 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 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. You can get statistics specific to the Application Service if you have provisioned AVR. Otherwise, you can always get object-level statistics.

Object-level statistics

Use the following procedure to view statistics.

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.

Upgrading an Application Service from previous version of the iApp template

If you upgraded your BIG-IP system from a version prior to 11.4 and had an existing Application Service that used the f5.dns template from one of those previous versions, you will see a warning that the source template has changed. In version 11.4 and later, the f5.dns template has been significantly improved, and we strongly recommend you upgrade the source template to the new template available in v11.4.

When you upgrade to the current template version, the iApp retains all of your settings for use in the new template. You will notice the location of the questions are different in the new version of the template, most questions are asked in a different way, and BIG-IP WebAccelerator is now called BIG-IP Application Acceleration Manager. There are also many more options you can configure in the new version of the template.

To upgrade an Application Service to the current version of the template

1. On the Main tab, expand **iApp** and then click **Application Services**.
2. From the list, click the name of the application service you created using the f5.dns template. You'll see a warning icon in the Template Validity column.
3. On the Menu bar, click **Reconfigure**.
4. In the Template Options section, from the **Do you want to upgrade this template** question, select **Yes**.
5. Without changing any settings, click the **Finished** button. The system creates an application service object with only the new template object in the Component view.

> ***Warning***
>
> *Your application will be offline from now until you complete the process in step 9*

6. On the Menu bar, click **Reconfigure**. Note the Template options section with inline help and configuration mode options. A number of additional questions appear if you select Advanced mode.
7. In the **Virtual Server and Pool** section, in the **What FQDNs will clients use to access the servers** question, you must add the host name.
8. No additional changes are necessary, but you may modify any of the other settings as applicable for your implementation. Use the inline help and this deployment guide for information on specific settings.
9. Click **Finished**. The upgrade is now complete and all applicable objects appear in the Component view.

Appendix: Manual configuration table

We strongly recommend using the iApp template to configure the BIG-IP system for DNS traffic. This table contains a list of BIG-IP 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 (*Main tab-->Local Traffic -->Monitors*)	***Name***	Type a unique name
	Type	**DNS**
	Interval	**30** (recommended)
	Timeout	**91** (recommended)
	Query Name	Type the host name you want to send the DNS server. The BIG-IP system sends a request to the DNS servers for this host name to determine server availability.
	Query Type	Choose whether you want to use an A or AAAA record to check the health of the DNS servers.
	Receive String	Type the IP address you expect to receive from the DNS servers as a response to the query name request above. If you leave this field blank, the monitor marks the server up if the DNS response code is no-error
Pool (*Main tab-->Local Traffic -->Pools*)	***Name***	Type a unique name
	Health Monitor	Select the monitor you created above
	Slow Ramp Time[1]	**300**
	Load Balancing Method	Choose a load balancing method. We use **Least Connections (member)**
	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**
	DNS (*Profiles-->Protocol*)	Name: Type a unique name
		Parent Profile: **udp**
		Datagram LB: Check the box to **Enable** Datagram LB
Virtual Servers (*Main tab-->Local Traffic -->Virtual Servers*	**UDP**	
	Name	Type a unique name.
	Destination Address	Type the IP Address for the virtual server
	Service Port	**53**
	Protocol	**UDP**
	Protocol Profile (Client)	Select the DNS profile you created
	Source Address Translation [2]	**Auto Map** (optional; see footnote [2])
	Default Pool	Select the pool you created
	TCP *(Optional: Only used when the response exceeds 512 bytes or for zone transfers)*	
	Name	Type a unique name.
	Destination Address	Type the IP Address for the virtual server
	Service Port	**53**
	Protocol Profile (Client)	If most clients are connecting over the WAN, select the WAN optimized TCP profile you created. If most clients are on the LAN, select the LAN optimized profile you created.
	Protocol Profile (Server)	If most connections between the BIG-IP and the servers are over the LAN, select the LAN optimized TCP profile you created. If most connections are over the WAN, select the WAN optimized profile you created.
	Source Address Translation [2]	**Auto Map** (optional; see footnote [2])
	Default Pool	Select the pool you created

[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.*

Glossary

application service
iApps application services use an *iApp Template* to guide users through configuring new BIG-IP® system configurations. An application service lets an authorized user easily and consistently deploy complex BIG-IP® system configurations just by completing the information required by the associated template. Every application service is attached to a specific configuration and cannot be copied the way that iApps templates can.

iApp Template
iApps templates create configuration-specific forms used by application services to guide authorized users through complex system configurations. The templates provide programmatic, visual layout and help information. Each new application service uses one of the templates to create a screen with fields and help that guide the user through the configuration process and creates the configuration when finished.

iApps templates allow users to customize by either modifying an existing template or creating one from scratch. Users can create scratch-built templates using either the iApps Templates screen or any text-editing software.

configuration utility
The Configuration utility is the browser-based application that you use to configure the BIG-IP system.

custom profile
A custom *profile* is a profile that you create. A custom profile can inherit its default settings from a parent profile that you specify. See also parent profile.

health monitor
A health monitor checks a node to see if it is up and functioning for a given service. If the node fails the check, it is marked down. Different monitors exist for checking different services.

iRule
An iRule is a user-written script that controls the behavior of a connection passing through the BIG-IP system. iRules™ are an F5 Networks feature and are frequently used to direct certain connections to a non-default load balancing pool. However, iRules can perform other tasks, such as implementing secure network address translation and enabling session persistence. You can attach iRules you created to your DNS application service in the advanced configuration mode.

load balancing method
A load balancing method or algorithm is a particular method of determining how to distribute connections across a *load balancing pool*. There are several different load balancing methods on the BIG-IP system. If you are working with servers that differ significantly in processing speed and memory, you might want to use a method such as Ratio or Weighted Least Connections.

Load balancing calculations can be localized to each pool (member-based calculation) or they may apply to all pools of which a server is a member (node-based calculation). For detailed information, see the product documentation.

See the table on the following page for a description of most load balancing methods.

Method	Description	When to use
Round Robin	Round Robin mode passes each new connection request to the next server in line, eventually distributing connections evenly across the array of machines being load balanced.	Round Robin mode works well in most configurations, especially if the equipment that you are load balancing is roughly equal in processing speed and memory.
Ratio (member) **Ratio (node)**	The LTM distributes connections among pool members in a static rotation according to ratio weights you define. The number of connections each system receives over time is proportionate to the ratio weight you defined for each pool member. You set a ratio weight when you add each pool member in the iApp.	These are static load balancing methods, basing distribution on user-specified ratio weights that are proportional to the capacity of the servers.

Method	Description	When to use
Dynamic Ratio (member) **Dynamic Ratio (node)**	The Dynamic Ratio methods select a server based on various aspects of real-time server performance analysis. These methods are similar to the Ratio methods, except the ratio weights are system-generated, and the values of the ratio weights are not static. These methods are based on continuous monitoring of the servers, and the ratio weights are therefore continually changing.	The Dynamic Ratio methods are used specifically for load balancing traffic to RealNetworks® RealSystem® Server platforms, Windows® platforms equipped with Windows Management Instrumentation (WMI), or any server equipped with an SNMP agent such as the UC Davis SNMP agent or Windows 2000 Server SNMP agent. Note: To implement Dynamic Ratio load balancing, you must first install and configure the necessary server software for these systems, and then install the appropriate performance monitor.
Fastest (node) **Fastest (application)**	The Fastest load balancing mode load balances based upon the number of outstanding Layer 7 requests to a pool member and the number of open L4 connections.	The Fastest methods are useful in environments where nodes are distributed across separate logical networks.
Least Connections (member) **Least Connections (node)**	The Least Connections load balancing mode is a dynamic load balancing algorithm that distributes connections to the server that is currently managing the fewest open connections at the time the new connection request is received.	The Least Connections methods function best in environments where the servers have similar capabilities. Otherwise, some amount of latency can occur. If you have servers with varying capacities, consider using the Weighted Least Connections methods instead.
Weighted Least Connections (member) **Weighted Least Connections (node)**	Specifies that the system passes a new connection to the pool member that is handling the lowest percentage of the specified maximum number of concurrent connections allowed. This mode requires that you specify a value for the connection-limit option for all members of the pool.	This mode works best in environments where the servers or other equipment you are load balancing have different but quantified capability limits.
Observed (member) **Observed (node)**	With the Observed methods, nodes are ranked based on the number of connections. The Observed methods track the number of Layer 4 connections to each node over time and create a ratio for load balancing	The need for the Observed methods is rare, and they are not recommended for large pools.
Predictive (member) **Predictive (node)**	The Predictive methods use the ranking methods used by the Observed methods. However, with the Predictive methods, LTM analyzes the trend of the ranking over time, determining whether a nodes performance is currently improving or declining. The servers with performance rankings that are currently improving receive a higher proportion of the connections.	The need for the Predictive methods is rare, and they are not recommended for large pools.
Least Sessions	The Least Sessions method selects the server that currently has the least number of entries in the persistence table. Use of this load balancing method requires that the virtual server reference a type of profile that tracks persistence connections, such as the Source Address Affinity or Universal profile type. Note: The Least Sessions methods are incompatible with cookie persistence.	The Least Sessions method works best in environments where the servers or other equipment that you are load balancing have similar capabilities.

load balancing pool

A load balancing pool is a logical set of devices, such as DNS servers, that you group together to receive and process traffic. Instead of sending client traffic to the destination IP address specified in the client request, Local Traffic Manager sends the request to any of the servers that are members of that pool. This helps to efficiently distribute the load on your server resources.

profile

Profiles are a configuration tool that you can use to affect the behavior of certain types of network traffic. More specifically, a profile is an object that contains settings with values, for controlling the behavior of a particular type of network traffic. Profiles also provide a way for you to enable connection and session persistence, and to manage client application authentication.

self IP address

Self IP addresses are the IP addresses owned by the BIG-IP system that you use to access the internal and external VLANs.

SNAT
A SNAT (Secure Network Address Translation) is a feature that defines a routable alias IP address that one or more nodes can use as a source IP address when making connections to hosts on the external network.

SNAT pool
A SNAT pool is a pool of translation addresses that you can map to one or more original IP addresses. Translation addresses in a SNAT pool are not self IP addresses.

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 port. This is the address clients use to connect to the DNS servers (or a FQDN resolves to this address). The BIG-IP intercepts the client request, and then directs the traffic according to your configuration instructions.

VLAN
A VLAN is a logical grouping of interfaces connected to network devices. You can use a VLAN to logically group devices that are on different network segments. Devices within a VLAN use Layer 2 networking to communicate and define a broadcast domain.

Document Revision History

Version	Description	Date
1.0	New Deployment Guide for BIG-IP v11.4	06-11-2013
1.1	- Added support for BIG-IP v11.4.1 and 11.5. - The updated iApp template in 11.5 contains the following fixes and additions: * The iApp no longer displays an error when configuring a SNAT Pool. * The iApp no longer attempts to enable TCP request queuing on the UDP virtual server.	01-31-2014
1.2	- Added support for BIG-IP v11.5.1. - Added three new entries to the manual configuration appendix for the health monitor.	06-02-2014
1.3	- Added support for BIG-IP v11.5.1.	08-25-2014
1.4	- Added support for BIG-IP v11.6. - Corrected the *Appendix: Manual configuration table on page 15*. There were previously a number of objects that did not apply to this configuration.	05-15-2015

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