Deployment Guide

LDAP Servers

Important: This guide has been archived. While the content in this guide is still valid for the products and versions listed in the document, it is no longer being updated and may refer to F5 or third party products or versions that have reached end-of-life or end-of-support. For a list of current guides, see https://f5.com/solutions/deployment-guides.

Deploying the BIG-IP System v11 with LDAP Servers

What's inside:

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

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

Why F5?

The BIG-IP system provides a number of ways to accelerate, optimize, and scale LDAP server deployments. The BIG-IP LTM uses an advanced health monitor that logs on to an LDAP server and performs a search query to a specific directory level to ensure traffic is only sent to available LDAP servers.

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	v11.0 - 11.3.x

Important: *Make sure you are using the most recent version of this deployment guide, available at http://www.f5.com/pdf/deployment-guides/ldap-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 LDAP acts as the single-point interface for building, managing, and monitoring your LDAP 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.

Document Version
1.2

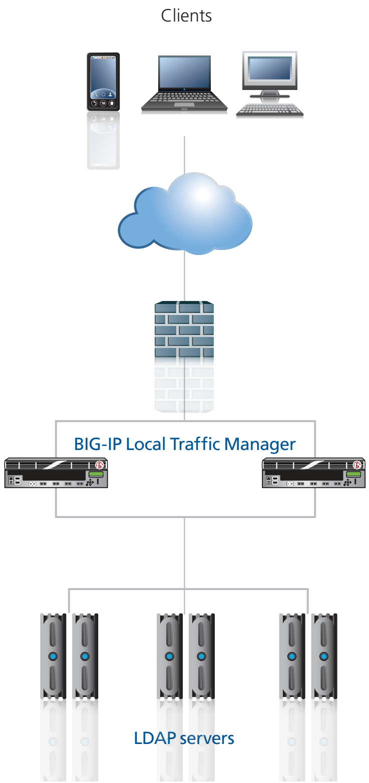
Prerequisites and configuration notes

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 - 11.3.x. If you are using a previous or later 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 or later versions. There is an updated iApp and guide for 11.4 and later.
- This deployment guide provides guidance for using the iApp for LDAP found in version 11.0 - 11.3.x. For advanced users extremely familiar with the BIG-IP, there are manual configuration tables at the end of this guide. However, we strongly recommend using the iApp template.
- The BIG-IP health monitor created by the template requires an LDAP user account. To check the health of the servers, the monitor uses this account to log in to LDAP and conduct a search query at a specific level in the directory. We recommend you create a new LDAP user account for this health monitor.
- If you are using the BIG-IP system to offload SSL, we assume you have already obtained an SSL certificate and key, and it is installed on the BIG-IP LTM system.
- This guide does not contain information on configuring LDAP servers. See your LDAP 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 LDAP servers. This diagram shows a logical configuration example with a redundant pair of BIG-IP LTM devices in front of a group of LDAP servers.



Preparation Worksheet

In order to use the iApp for LDAP, 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	SSL Offload	Pool Members	Sync/Failover Groups*	TCP request queuing*	WAN or LAN clients
IP address you will use for the LTM virtual server: FQDN that will resolve to the virtual server address:	*Offloading SSL?* Yes | No If offloading SSL, import a certificate and key into the BIG-IP LTM before running the template. Certificate: Key:	LDAP server IP addresses: 1: 2: 3: 4: 5: 6: 7: 8: 9: 10: Port used by LDAP:	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:	If using TCP request queuing, you should know the queue length and timeout, as well as the connection limit for the node. Request queue length: Timeout: Node Connection limit:	Most clients connecting through BIG-IP to LDAP are coming over a: LAN WAN

Health Monitor
User name with access to LDAP. Must be a Distinguished Name: Password associated with the user name: Level in the directory do you want to begin searching (for example ou=users,dc=siteserver,dc=com): Search query you want the server to return results for:

* *Optional*

Configuring the BIG-IP iApp for LDAP

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

Getting Started with the iApp for LDAP

To begin the LDAP 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 **LDAP-server_**.
5. From the **Template** list, select **f5.ldap**.
   The LDAP 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 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 LDAP 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 LDAP 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 LDAP 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 that the BIG-IP is configured as the gateway to the client networks (usually the default gateway) on the LDAP 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 LDAP servers -- where the BIG-IP virtual server(s) and the LDAP 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.

SSL Encryption questions

Before running the template you should have already imported a certificate and key onto the BIG-IP system. While the BIG-IP system does include a self-signed SSL certificate that can be used internally or for testing, we strongly recommend importing a certificate and key issued from a trusted Certificate Authority.

For information on SSL certificates on the BIG-IP system, see the online help or the *Managing SSL Certificates for Local Traffic* chapter in the ***Configuration Guide for BIG-IP Local Traffic Manager*** *available at http://support.f5.com/kb/en-us.html.*

To configure the BIG-IP to offload SSL, select **Yes** from the list.

1. **Certificate**
   Select the certificate for you imported for the LDAP servers from the certificate list.
2. **Key**
   Select the associated key from the list.

Server Pool, Load Balancing, and Service Monitor questions

In this section, you add the LDAP 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 LDAP 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 LDAP server (the default port is 389). You can

➲ **Important**
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

optionally add a Connection Limit (see note on the left). Click **Add** to add additional servers to the pool.

4. **TCP Request Queuing**
   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 in accordance with defined conditions until capacity becomes available. For more information on TCP Request Queuing, see the *New Features Guide for BIG-IP Version 11*, available on Ask F5.

   If you want the BIG-IP to queue TCP requests, select **Yes** from the list. Additional options appear.

   a. Type a queue length in the box. Leave the default of 0 for unlimited.

   b. Type a number of milliseconds for the timeout value.

5. **Health Monitor**
   Choose **Create New Monitor** unless you have already made a health monitor on the LTM for the LDAP devices.

6. **User Account**
   The health monitor requires an LDAP user account, which the BIG-IP uses to log on to the server and go to a specific level in the directory to conduct a search. You must specify the user name as a LDAP Distinguished Name (such as cn=joe,dc=siterequest,dc=com).

Password

Type the password for the user name you entered above.

Warning: *The Password cannot contain a hash (#) character.*

7. **Directory Level**
   Type the level in the directory that you want the monitor to begin searching (for example, ou=users,dc=siterequest,dc=com).

8. **Search Query**
   Type the search query you want the monitor to use. The health check is successful if the query returns with a valid value, otherwise the node will be marked down.

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.

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 LDAP implementation.

Next steps

After completing the iApp Template, the BIG-IP Application Services page opens for the LDAP service you just created. To see the list of all the configuration objects created to support LDAP, on the Menu bar, click **Components**. The complete list of all LDAP 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 LDAP 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). As a safer option, the 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 LDAP 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 LDAP configuration objects created by the iApp template.

Object-level statistics
Use the following procedure to view object-level 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.

Appendix: Manual configuration table

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

This 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 (*Main tab-->Local Traffic -->Monitors*)	***Name***	Type a unique name	
	Type	**LDAP**	
	Interval	**10** (recommended)	
	Timeout	**31** (recommended)	
	User Name	You must specify the user name as a LDAP Distinguished Name (such as cn=joe,dc=siterequest,dc=com)	
	Password	Type the associated password. **Warning:** *The password cannot contain a hash (#) character*	
	Base	Type the level in the directory that you want the monitor to begin searching (for example, ou=users,dc=siterequest,dc=com)	
	Filter	Type the search query you want the monitor to use. The health check is successful if the query returns with a valid value, otherwise the node will be marked down.	
Pool (*Main tab-->Local Traffic -->Pools*)	***Name***	Type a unique name	
	Health Monitor	Select the monitor created by the template.	
	Slow Ramp Time[1]	**300**	
	Load Balancing Method	Choose a load balancing method. We use the default **Round Robin**	
	Address	Type the IP Address of the LDAP nodes	
	Service Port	**389** (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**
	Persistence (*Profiles-->Persistence*)	Name	Type a unique name
		Persistence Type	**Source Address Affinity**
	Client SSL[2] (*Profiles-->SSL*)	Name	Type a unique name
		Parent Profile	**clientssl**
		Certificate and Key	Select the Certificate and Key you imported from the associated list
Virtual Servers (*Main tab-->Local Traffic -->Virtual Servers*)	***Name***	Type a unique name	
	Address	Type the IP Address for the virtual server	
	Service Port	**389** (**636** if offloading SSL)	
	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 Pool[3]	**Automap** (optional; see footnote [3])	
	Default Pool	Select the pool you created above	
	Persistence Profile	Select the Persistence profile you created above	

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

[2] Only necessary if you are offloading SSL

[3] *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	Date
1.0	New Version	N/A
1.1	The manual configuration table incorrectly listed HTTP as the monitor type. This has been corrected to LDAP. The rest of the settings in the monitor were correct. The iApp template created the correct LDAP monitor.	08-23-2013
1.2	- Added warnings in the iApp walkthrough and the manual configuration tables about not using hash (#) characters in the LDAP Password you choose for the health monitor. - Added to the note in the prerequisites about the maximum version of the BIG-IP system this guide applies to (11.3.x). An updated version of the iApp template and the deployment guide are available in 11.4 and later.	06-06-2014

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