DEPLOYMENT GUIDE
Version 1.0

Deploying the BIG-IP LTM with the Zimbra Open Source Email and Collaboration Suite

Table of Contents

Deploying the BIG-IP LTM with the Zimbra Open Source Email and Collaboration Suite

Deploying the BIG-IP LTM with the Zimbra Open Source Email and Collaboration Suite

Welcome to the F5 deployment guide for Zimbra. This guide contains detailed procedures on configuring the BIG-IP Local Traffic Manager (LTM) with the different components of Zimbra v6.

Zimbra is a next-generation collaboration server that provides organizations greater overall flexibility and simplicity with integrated email, contacts, calendaring, sharing and document management plus mobility and desktop synchronization to users on any computer.

For more information on Zimbra, see ***http://www.zimbra.com/***.

For more information on the F5 devices included in this guide, see ***http://www.f5.com/products/***.

Prerequisites and configuration notes

The following are prerequisites and configuration notes for this deployment:

- We strongly recommend offloading SSL on the BIG-IP LTM, therefore, we recommend setting up Zimbra services on encrypted ports.
- In typical deployments, individual Zimbra services are located on their own servers. In these cases, in order to take advantage of high availability, the BIG-IP LTM virtual server name or address should be used in configuring the Zimbra Instances (for example, installing a new IMAP server, the LDAP virtual server on BIG-IP should be used instead of the LDAP server's direct address).

Product versions and revision history

Product and versions tested for this deployment guide:

Product Tested	Version Tested
BIG-IP LTM	v10.2
Zimbra Open Source Email and Collaboration Suite	v6

Revision history:

Document Version	Description
1.0	New deployment guide

Configuration example

Zimbra is a full featured Enterprise ready mail, calendar and messaging solution that can be installed in a variety of configurations. For greatest scalability and high availability, functional pieces of Zimbra are typically installed on separate servers.

In our configuration, we have configured four groups of servers (pools) that are fronted by BIG-IP virtual servers. Web servers, MTAs, IMAP/POP3 and LDAP servers are separated on their individual servers. By using this type of separation, additional servers can be added if capacity is required.

For each component, a BIG-IP virtual server offloads SSL and provides TCP optimization for incoming clients. By configuring the Zimbra components with the BIG-IP virtual IP address, additional high availability can be created and maintained with the Zimbra configuration itself.

In this document we detail all configuration procedures required to monitor Zimbra, but do not detail the installation of Zimbra software itself. Refer to your Zimbra product documentation for this information.

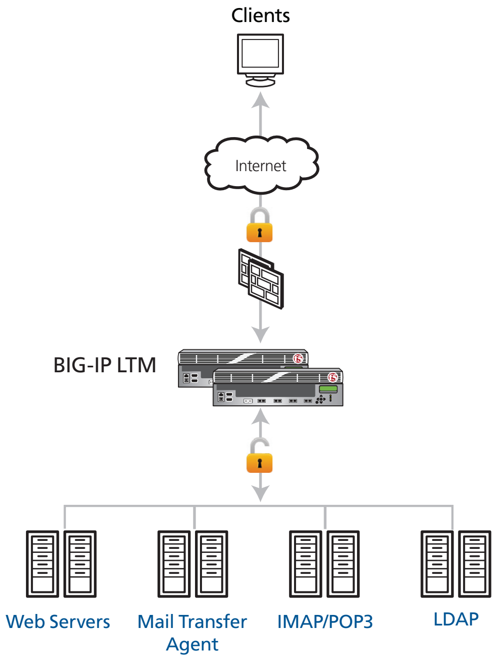


***Figure 1** Logical configuration example*

◆ **Note**

Communication between servers can go through the BIG-IP LTM to take advantage of high availability services. Simply configure your Zimbra multi-server installation with the Virtual IP Address on BIG instead of direct server host names.

Using the configuration table

The table on the following page contains a list of the BIG-IP configuration objects that are a part of this deployment. It is provided for reference, but advanced users extremely familiar with the BIG-IP system can use it rather than relying on the step-by-step configuration procedures that follow. If you find the table does not contain enough information for you to configure an individual object, see the appropriate detailed section.

In the following table, we have included optional setup information for environments that do not wish to offload encryption. Because this is an atypical deployment we have left this section as optional.

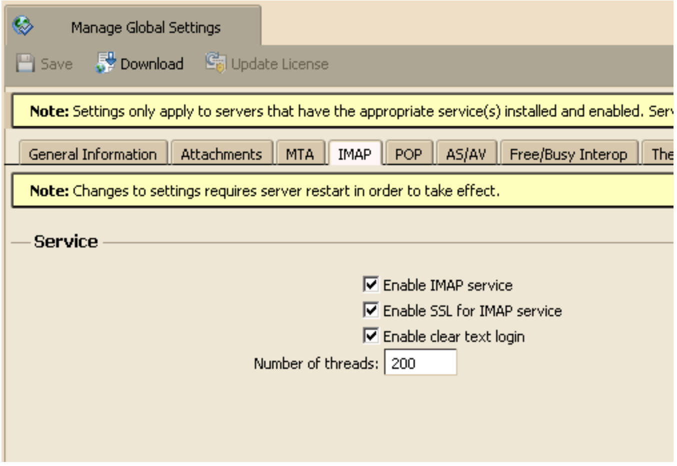
Zimbra Role/Service	Monitor	Pool Port	Profiles	VIP Port/Notes
HTTPS	HTTP	80	- HTTP: *HTTP Acceleration* *Redirect Rewrite*: **All** *Insert XForwarded For*: **Enabled** - TCP x 2: LAN and WAN optimized - Client SSL (optional) - OneConnect	Port 443 *SNAT Pool*: **Automap**
IMAP	IMAP	143	- TCP x 2: LAN and WAN optimized - Persistence: Source Address Affinity - Client SSL (optional)	Port 143 *SNAT Pool*: **Automap**
POP	POP3	110	- Persistence: Source Address Affinity - Client SSL (optional)	Port 110 *SNAT Pool*: **Automap**
Mail Transfer Agent: non-TLS	SMTP	25	- TCP x 2: LAN and WAN optimized - Client SSL (optional)	Port 25 *SNAT Pool*: **Automap**
LDAP	LDAP	389	- TCP WAN Optimized - Client SSL (optional)	Port 389 *SNAT Pool*: **Automap**
Optional Roles and Services that are necessary if not offloading on the BIG-IP LTM				
IMAPS	IMAP	993	- TCP x 2: LAN and WAN optimized - Persistence: Source Address Affinity	Port 993 *SNAT Pool*: **Automap**
POP3S	POP3	995	- Persistence: Source Address Affinity	Port 995 *SNAT Pool*: **Automap**
Mail Transfer Agent: TLS	SMTP	465	- TCP x 2: LAN and WAN optimized	Port 465 *SNAT Pool*: **Automap**
LDAPS	LDAPS	636	- TCP WAN Optimized	Port 636 *SNAT Pool*: **Automap**

Modifying the Zimbra configuration for the BIG-IP health monitors

The first task is to modify the Zimbra Server global settings so the BIG-IP LTM health monitors you create are able to log in and verify that the devices are not only up, but operating properly.

To modify the Zimbra configuration

1. Log into the Zimbra Administration console.
2. From the left navigation pane, in the **Configuration** section, select **Global Settings**.
3. In the main pane, click the **IMAP** tab, and then check the **Enable clear text login** box.



Note: Settings only apply to servers that have the appropriate service(s) installed and enabled. Serv

Note: Changes to settings requires server restart in order to take effect.

Service

☑ Enable IMAP service
☑ Enable SSL for IMAP service
☑ Enable clear text login
Number of threads: 200

Figure 2 *Global settings - IMAP tab*

4. In the main pane, click the **POP** tab, and then check the **Enable clear text login** box.
5. You may need to restart the server.

This completes the Zimbra configuration changes. Continue with the following section.

Configuring the BIG-IP LTM for Zimbra

In this section, we configure the BIG-IP LTM for the Zimbra roles and services.

Creating the health monitors

In this section, we configure each of the health monitors for the various Zimbra roles/services.

This section contains procedures for the following five health monitors:

- HTTP
- IMAP
- SMTP
- POP3
- LDAP
- *Optional:* TCP

Creating the HTTP monitor

Use the following procedure to create the HTTP monitor.

To configure a health monitor

1. On the Main tab, expand **Local Traffic**, and then click **Monitors**. The Monitors screen opens.
2. Click the **Create** button. The New Monitor screen opens.
3. In the **Name** box, type a name for the Monitor. In our example, we type **zimbra-HTTP**.
4. From the **Type** list, select **HTTP**. The HTTP Monitor configuration options appear.
5. In the Configuration section, in the **Interval** and **Timeout** boxes, type an Interval and Timeout. We recommend at least a 1:3 +1 ratio between the interval and the timeout. In our example, we use a **Interval** of **30** and a **Timeout** of **91**.
6. ***Optional:*** In the **Send String** and **Receive String** sections, you can add Send and Receive strings specific to the device being checked. This enables a much more granular health check.

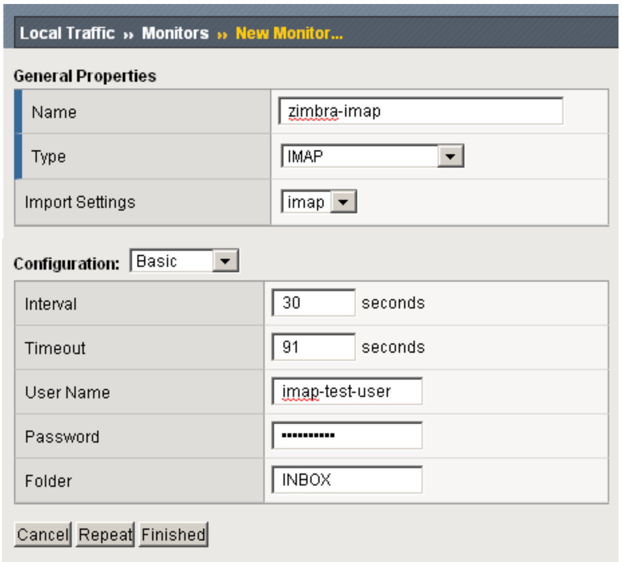
   If the page you are requesting in the Send String requires authentication, type a user name and password in the appropriate boxes.
7. Click the **Finished** button.

Creating the IMAP monitor

The next monitor we create is an IMAP monitor. For this monitor, you need an IMAP user account. We recommend creating a new IMAP user to be used solely for the purpose of this health check.

To create the IMAP health monitor

1. On the Main tab, expand **Local Traffic**, click **Monitors** and then click the **Create** button. The New Monitor screen opens.
2. In the **Name** box, type a name for the Monitor. In our example, we type **zimbra-IMAP**.
3. From the **Type** list, select **IMAP.**
   For advanced configuration options, from the **Configuration** list, select **Advanced**.
4. In the Configuration section, in the **Interval** and **Timeout** boxes, type an Interval and Timeout. In our example, we use a **Interval** of **30** and a **Timeout** of **91.**
5. In the **User Name** box, type a user name with a valid IMAP account. We recommend a user account just for this monitor.
6. In the **Password** box, type the corresponding password.
7. All other settings are optional, configure as applicable.
8. Click the **Finished** button.



General Properties

Name	zimbra-imap
Type	IMAP
Import Settings	imap

Configuration: Basic

Interval	30 seconds
Timeout	91 seconds
User Name	imap-test-user
Password	••••••••••
Folder	INBOX

Figure 3 *IMAP monitor configuration*

Creating the POP3 monitor

Next, we create the POP3 monitor. As with IMAP, we recommend creating a POP3 user account to be used specifically for this health monitor.

To create the POP3 health monitor

1. On the Main tab, expand **Local Traffic**, click **Monitors** and then click the **Create** button. The New Monitor screen opens.
2. In the **Name** box, type a name for the Monitor. In our example, we type **zimbra-POP3**.
3. From the **Type** list, select **POP3.**

   *For advanced configuration options, from the **Configuration** list, select **Advanced**.*
4. In the Configuration section, in the **Interval** and **Timeout** boxes, type an Interval and Timeout. In our example, we use a **Interval** of **30** and a **Timeout** of **91.**
5. In the **User Name** box, type a user name of a user with a valid POP3 account. We recommend creating a user account just for this monitor.
6. In the **Password** box, type the corresponding password.
7. All other settings are optional, configure as applicable.
8. Click the **Finished** button.

Creating the SMTP monitor

Next, we create the SMTP monitor for the Mail Transfer Agent devices.

To create the SMTP health monitor

1. On the Main tab, expand **Local Traffic**, click **Monitors** and then click the **Create** button. The New Monitor screen opens.
2. In the **Name** box, type a name for the Monitor. In our example, we type **zimbra-SMTP**.
3. From the **Type** list, select **SMTP.**

   *For advanced configuration options, from the **Configuration** list, select **Advanced**.*
4. In the Configuration section, in the **Interval** and **Timeout** boxes, type an Interval and Timeout. In our example, we use a **Interval** of **30** and a **Timeout** of **91.**
5. In the **Domain** box, type the domain name you want the monitor to check. In our example we type **smtp.zimbra.example.com**.
6. All other settings are optional, configure as applicable.
7. Click the **Finished** button.

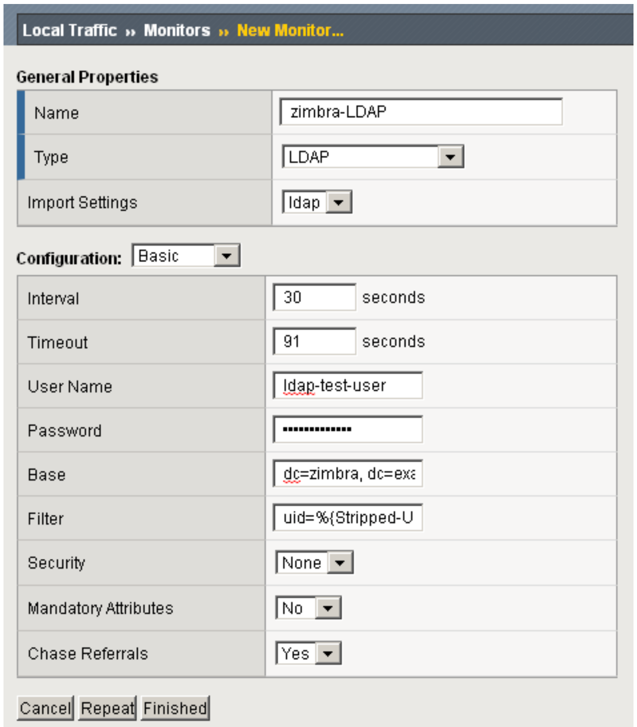
Creating the LDAP monitor

The next monitor we create is an LDAP monitor.

To create the LDAP health monitor

1. On the Main tab, expand **Local Traffic**, click **Monitors** and then click the **Create** button. The New Monitor screen opens.
2. In the **Name** box, type a name for the Monitor. In our example, we type **zimbra-LDAP**.
3. From the **Type** list, select **LDAP.**
4. In the Configuration section, in the **Interval** and **Timeout** boxes, type an Interval and Timeout. In our example, we use a **Interval** of **30** and a **Timeout** of **91.**
5. In the **Base** box, type a base. The base specifies the location in the LDAP tree from which the monitor starts the health check. In our example, we type **dc=zimbra, dc=example,dc=com**.
6. In the **Filter** box, type a filter. The filter specifies an LDAP key for which the monitor searches. We recommend **uid=%{Stripped-User-Name:-%{User-Name}}**
7. Leave all other settings at the defaults (see Figure 4, on page 9).
8. Click the **Finished** button.
9. *Optional:* If you are not using the BIG-IP LTM to offload SSL, repeat this procedure to create an LDAPS monitor, with the following additions:
   - Give the monitor a unique name.
   - From the **Configuration** list, select **Advanced**.
   - From the **Security** list, select **SSL** or **TLS**, whichever method is appropriate for your configuration

For a complete guide on best practices for LDAP monitoring, see ***http://support.f5.com/kb/en-us/solutions/public/9000/300/sol9311.html?sr=10491565***



General Properties

Name	zimbra-LDAP
Type	LDAP
Import Settings	ldap

Configuration: Basic

Interval	30 seconds
Timeout	91 seconds
User Name	ldap-test-user
Password	•••••••••••••
Base	dc=zimbra, dc=exa
Filter	uid=%{Stripped-U
Security	None
Mandatory Attributes	No
Chase Referrals	Yes

Figure 4 *LDAP monitor configuration*

Creating a TCP monitor (optional)

The final monitor we create in this configuration is a basic TCP monitor that is used if you are ***not*** using the BIG-IP to offload SSL/TLS.
Only create this monitor if you are not using the BIG-IP LTM to offload SSL/TLS.

To create the TCP health monitor

1. On the Main tab, expand **Local Traffic**, click **Monitors** and then click the **Create** button. The New Monitor screen opens.
2. In the **Name** box, type a name for the Monitor. In our example, we type **zimbra-TCP**.
3. From the **Type** list, select **TCP.**
4. In the Configuration section, in the **Interval** and **Timeout** boxes, type an Interval and Timeout. In our example, we use a **Interval** of **30** and a **Timeout** of **91.**
5. Modify any of the other settings as applicable for your configuration. In our example, we leave the defaults.
6. Click **Finished**.

This completes the health monitor configuration.

Creating the pools

In this section, we create the load balancing pools.

◆ **Tip**

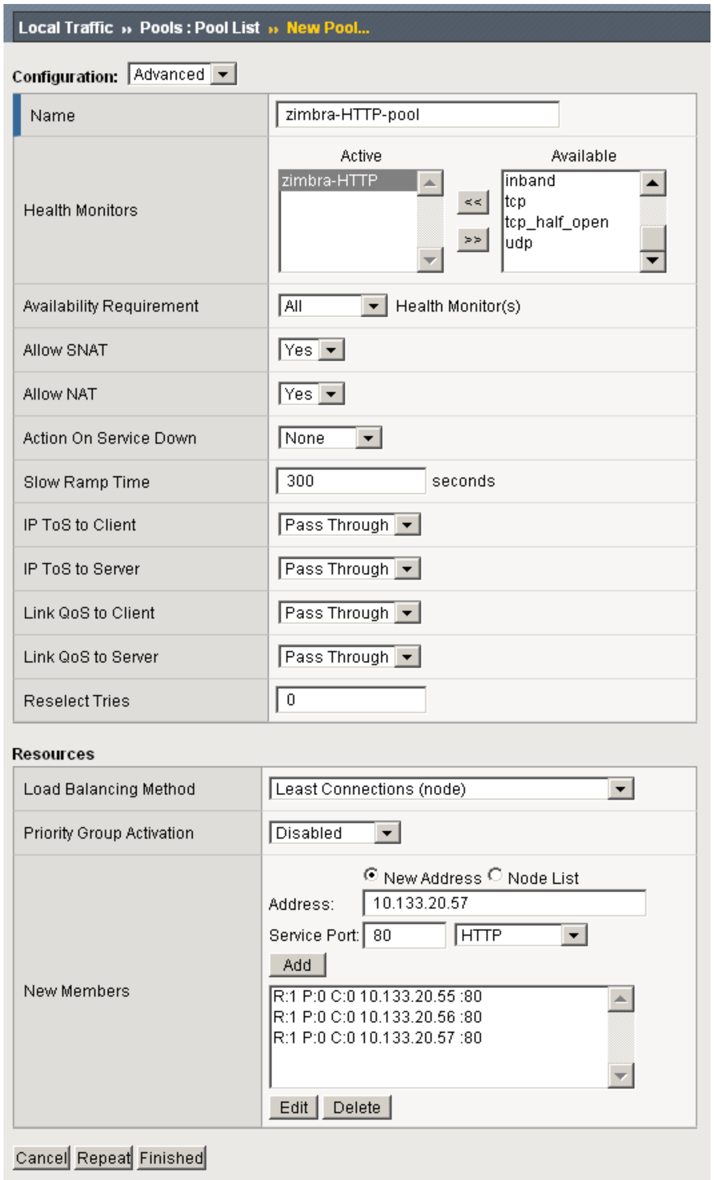
Before creating the pools, you should know if you are going to offload SSL on the BIG-IP system. If you are offloading SSL, you do not need to create separate pools for services like IMAPS and POP3S.

Creating the HTTP pool

The first pool we create is for the HTTP members.

To create the HTTP pool

1. On the Main tab, expand **Local Traffic**, and then click **Pools**. The Pool screen opens.
2. Click the **Create** button. The New Pool screen opens.
3. From the Configuration list, select **Advanced**.
4. In the **Name** box, type a name for your pool. In our example, we use **zimbra-HTTP-pool**.
5. In the **Health Monitors** section, select the name of the monitor you created in *Creating the HTTP monitor*, on page 5, and click the Add (<<) button. In our example, we select **zimbra-HTTP**.
6. In the **Slow Ramp Time** box, type **300**. We set the Ramp Time in order to ensure that if a pool member becomes available after maintenance or a new member is added, the Least Connections load balancing algorithm does not send all new connections to that member (a newly available member will always have the least number of connections).
7. From the **Load Balancing Method** list, choose your preferred load balancing method (different load balancing methods may yield optimal results for a particular network). In our example, we select **Least Connections (node)**.
8. From the New Members section, in the **Address** box, type the IP address of one of the devices. In our example, we type **10.133.20.55**
9. In the **Service Port** box, type the service number you want to use for this device, or specify a service by choosing a service name from the list. In our example, we type **80**.
10. Click the **Add** button to add the member to the list.
11. Repeat steps 8-10 for each server you want to add to the pool.
12. Click the **Finished** button (see Figure 5, on page 11).



Local Traffic » Pools : Pool List » New Pool...

Configuration: Advanced

Name	zimbra-HTTP-pool
Health Monitors	Active: zimbra-HTTP Available: inband, tcp, tcp_half_open, udp
Availability Requirement	All Health Monitor(s)
Allow SNAT	Yes
Allow NAT	Yes
Action On Service Down	None
Slow Ramp Time	300 seconds
IP ToS to Client	Pass Through
IP ToS to Server	Pass Through
Link QoS to Client	Pass Through
Link QoS to Server	Pass Through
Reselect Tries	0

Resources

Load Balancing Method	Least Connections (node)
Priority Group Activation	Disabled
New Members	● New Address ○ Node List Address: 10.133.20.57 Service Port: 80 HTTP Add R:1 P:0 C:0 10.133.20.55 :80 R:1 P:0 C:0 10.133.20.56 :80 R:1 P:0 C:0 10.133.20.57 :80 Edit Delete

Cancel Repeat Finished

Figure 5 New Pool configuration

Creating the IMAP pool(s)

Next, we create the IMAP pool.

To create the IMAP pool

1. On the main Pool screen, click **Create**.
2. From the Configuration list, select **Advanced**.
3. In the **Name** box, type a name. We type **zimbra-IMAP-pool**.

4. In the **Health Monitors** section, select the monitor you created in *Creating the IMAP monitor*, on page 6, and then click the Add (<<) button. We select **zimbra-IMAP**.
5. In the **Slow Ramp Time** box, type **300**.
6. From the **Load Balancing Method** list, choose a balancing method. We select **Least Connections (node)**.
7. From the New Members section, in the **Address** box, type the IP address of one of the devices. In our example, we type **10.133.30.55**
8. In the **Service Port** box, type **143**.
9. Click the **Add** button to add the member to the list.
10. Repeat steps 7-9 for each server you want to add to the pool.
11. Click the **Finished** button.
12. *Optional*: Only if you are ***not*** using the BIG-IP LTM to offload SSL, repeat this entire procedure for IMAPS with the following exceptions:
    - In step 3, give the pool a unique name, such as **zimbra-IMAPS-pool**.
    - In step 4, select the TCP monitor you created in *Creating a TCP monitor (optional)*, on page 9.
    - In step 8, in the **Service Port** box, type **993**.

Creating the POP3 pool(s)

Next, we create the POP3 pool.

To create the POP pool

1. On the main Pool screen, click **Create**.
2. From the Configuration list, select **Advanced**.
3. In the **Name** box, type a name. We type **zimbra-POP3-pool**.
4. In the **Health Monitors** section, select the monitor you created in *Creating the POP3 monitor*, on page 7, and then click the Add (<<) button. We select **zimbra-POP3**.
5. In the **Slow Ramp Time** box, type **300**.
6. From the **Load Balancing Method** list, choose a balancing method. We select **Least Connections (node)**.
7. From the New Members section, in the **Address** box, type the IP address of one of the devices. In our example, we type **10.133.40.55**
8. In the **Service Port** box, type **110**.
9. Click the **Add** button to add the member to the list.
10. Repeat steps 7-9 for each server you want to add to the pool.

11. Click the **Finished** button.
12. *Optional*: Only if you are ***not*** using the BIG-IP LTM to offload SSL, repeat this entire procedure for POPS with the following exceptions:

    - In step 3, give the pool a unique name, such as **zimbra-POPS-pool**.
    - In step 4, select the TCP monitor you created in *Creating a TCP monitor (optional)*, on page 9.
    - In step 8, in the **Service Port** box, type **995**.

Creating the Mail Transfer Agent pool(s)

Next, we create the Mail Transfer Agent (MTA) pool.

To create the MTA pool

1. On the main Pool screen, click **Create**.
2. From the Configuration list, select **Advanced**.
3. In the **Name** box, type a name. We type **zimbra-MTA-pool**.
4. In the **Health Monitors** section, select the monitor you created in *Creating the SMTP monitor*, on page 7, and then click the Add (**<<**) button. We select **zimbra-SMTP**.
5. In the **Slow Ramp Time** box, type **300**.
6. From the **Load Balancing Method** list, choose a balancing method. We select **Least Connections (node)**.
7. From the New Members section, in the **Address** box, type the IP address of one of the devices. In our example, we type **10.133.50.55**
8. In the **Service Port** box, type **25**.
9. Click the **Add** button to add the member to the list.
10. Repeat steps 7-9 for each server you want to add to the pool.
11. Click the **Finished** button.
12. *Optional*: Only if you are ***not*** using the BIG-IP LTM to offload TLS, repeat this entire procedure for MTA using TLS with the following exceptions:

    - In step 3, give the pool a unique name, such as **zimbra-MTA-TLS-pool**.
    - In step 4, select the TCP monitor you created in *Creating a TCP monitor (optional)*, on page 9.
    - In step 8, in the **Service Port** box, type **465**.

Creating the LDAP pool

Next, we create the pool for the LDAP devices.

To create the LDAP pool

1. On the main Pool screen, click **Create**.
2. From the Configuration list, select **Advanced**.
3. In the **Name** box, type a name. We type **zimbra-LDAP-pool**.
4. In the **Health Monitors** section, select the monitor you created in *Creating the LDAP monitor*, on page 8, and then click the Add (**<<**) button. We select **zimbra-LDAP**.
5. In the **Slow Ramp Time** box, type **300**.
6. From the **Load Balancing Method** list, choose a balancing method. We select **Least Connections (node)**.
7. From the New Members section, in the **Address** box, type the IP address of one of the devices. In our example, we type **10.133.60.55**
8. In the **Service Port** box, type **389**.
9. Click the **Add** button to add the member to the list.
10. Repeat steps 7-9 for each server you want to add to the pool.
11. Click the **Finished** button.
12. *Optional*: Only if you are ***not*** using the BIG-IP LTM to offload SSL, repeat this entire procedure for LDAPS with the following exceptions:
    - In step 3, give the pool a unique name, such as **zimbra-LDAPS-pool**.
    - In step 4, select the LDAPS monitor you created in the last step of *Creating the LDAP monitor*, on page 8.
    - In step 8, in the **Service Port** box, type **636**.

This is completes the pool configuration.

Creating the profiles

The next step is to create the profiles. A ***profile*** is an object that contains user-configurable settings for controlling the behavior of a particular type of network traffic, such as HTTP connections. Using profiles enhances your control over managing network traffic, and makes traffic-management tasks easier and more efficient.

In this deployment, we use the same profiles across Zimbra roles/services.

Creating the HTTP profile

The first profile we create is the HTTP profile.

To create a HTTP profile

1. On the Main tab, expand **Local Traffic**, and then click **Profiles**. The HTTP Profiles screen opens.
2. Click the **Create** button. The new HTTP Profile screen opens.
3. In the **Name** box, type a name for this profile. In our example, we type **zimbra-HTTP**.
4. From the Parent Profile list, select **http-acceleration**.
5. In the Settings section, check the Custom box for **Redirect Rewrite**, and from the **Redirect Rewrite** list, select **All.**
6. Check the Custom box next to **Insert XForwarded For**. Select **Enabled** from the list.
   Note on XForwarded For: It may be necessary for the BIG-IP system to insert the original client IP address in an HTTP header and configure the web server receiving the request to log the client IP address instead of the SNAT address. See SOL4816 (***https://support.f5.com/kb/en-us/solutions/public/4000/800/sol4816.html***) for more information on this header.
7. Click the **Finished** button.

Creating TCP profiles

The next task is to create the TCP profiles.

Creating the LAN optimized TCP profile

The first TCP profile we create is the LAN optimized profile.

To create a new LAN optimized TCP profile

1. On the Main tab, expand **Local Traffic**, and then click **Profiles**. The HTTP Profiles screen opens by default.
2. On the Menu bar, from the **Protocol** menu, select **TCP**.
3. Click the **Create** button. The New TCP Profile screen opens.

4. In the **Name** box, type a name for this profile. In our example, we type **zimbra-TCP-lan**.
5. From the **Parent Profile** list, select **tcp-lan-optimized**.
6. Modify any of the settings as applicable for your network. See the online help for more information on the configuration options. In our example, we leave the settings at their default levels.
7. Click the **Finished** button.

Creating the WAN optimized TCP profile

If your configuration uses various WAN links and your users are widely distributed, we recommend configuring the following WAN profile.

To create a new WAN optimized TCP profile

1. On the Main tab, expand **Local Traffic**, click **Profiles**, and then, on the Menu bar, from the **Protocol** menu, select **TCP**.
2. Click the **Create** button. The New TCP Profile screen opens.
3. In the **Name** box, type a name for this profile. In our example, we type **zimbra-TCP-wan**.
4. From the **Parent Profile** list, select **tcp-lan-optimized**.
5. Modify any of the settings as applicable for your network. See the online help for more information on the configuration options. In our example, we leave the settings at their default levels.
6. Click the **Finished** button.

Creating the persistence profile

The next task is to create a persistence profile. For Zimbra deployments, we use the Source Address Affinity persistence method.

To create a new persistence profile

1. On the Main tab, expand **Local Traffic**, click **Profiles**, and then, on the Menu bar, click **Persistence**.
2. Click the **Create** button.
3. In the **Name** box, type a name for this profile. In our example, we type **zimbra-persistence**.
4. From the **Persistence Type** list, select **Source Address Affinity**.
5. Modify any of the settings as applicable for your network. See the online help for more information on the configuration options.
6. Click the **Finished** button.

Creating the OneConnect Profile

OneConnect dramatically reduces the overhead of maintaining TCP connections between the BIG-IP LTM and the Zimbra servers.

To create a new OneConnect profile

1. On the Main tab, expand **Local Traffic**, and then click **Profiles**. The HTTP Profiles screen opens.
2. On the Menu bar, from the **Other** menu, click **OneConnect**. The Persistence Profiles screen opens.
3. In the upper right portion of the screen, click the **Create** button. The New HTTP Profile screen opens.
4. In the **Name** box, type a name for this profile. In our example, we type **zimbra-oneconnect**.
5. From the **Parent Profile** list, ensure that **oneconnect** is selected.
6. Modify any of the other settings as applicable for your network. In our example, we leave the settings at their default levels.
7. Click the **Finished** button.

Configuring the BIG-IP LTM for SSL offload

The BIG-IP LTM supports offloading of encryption (SSL/TLS) from servers for a number of protocols. In such configurations, all communication between the clients and the BIG-IP LTM take place over encrypted channels, and communication between the BIG-IP LTM and the Zimbra servers is unencrypted. Besides freeing the servers from the processing and memory overhead associated with encryption, and centralizing certificate management, the LTM is able to operate on the traffic using features such as acceleration profiles, iRules, and advanced persistence profiles.

Optionally, administrators can configure the BIG-IP LTM to re-encrypt traffic to the servers after initial decryption and processing; the LTM is still able to offer advanced traffic manipulation, but the servers are still burdened with encryption overhead. Such a configuration may be required in some organizations where network communications are mandated to be encrypted. Server-side SSL re-encryption is not covered in this guide.

◆ **Important**

This section is only necessary if you are offloading SSL on the BIG-IP LTM device. If not, continue with ***Creating the Zimbra virtual servers****, on page 20*

Importing keys and certificates

Before you can enable the BIG-IP LTM system to offload SSL traffic, you must install a SSL certificate and key on the BIG-IP LTM system. You will need one certificate and key pair for each FQDN (fully qualified domain name) that will be used for connectivity. In this guide, we show you how to use unique FQDNs for each service, each of which will require a certificate and key; we also show a configuration example where a single certificate/key pair is used for all services.

For this Deployment Guide, we assume that you already have obtained the required SSL certificates, but they are not yet installed on the BIG-IP LTM system. For information on generating certificates, or using the BIG-IP LTM system to generate a request for a new certificate and key from a certificate authority, see the ‘Managing SSL Traffic’ chapter in the ***Configuration Guide for Local Traffic Management***.

Once you have obtained a certificate, you can import this certificate into the BIG-IP LTM system using the Configuration utility. You can use the Import SSL Certificates and Keys screen only when the certificate you are importing is in Privacy Enhanced Mail (PEM) format.

To import a key or certificate

1. On the Main tab, expand Local Traffic.
2. Click **SSL Certificates**. This displays the list of existing certificates
3. In the upper right corner of the screen, click **Import**.
4. From the **Import Type** list, select the type of import (**Certificate** or **Key**).
5. In the **Certificate** (or **Key**) **Name** box, type a unique name for the certificate or key.
6. In the **Certificate** (or **Key**) **Source** box, choose to either upload the file or paste the text.
7. Click **Import**.
8. If you imported the certificate, repeat this procedure for the key.
9. Modify any of the settings as applicable for your network. See the online help for more information on the configuration options. In our example, we leave the settings at their default levels.
10. Click the **Finished** button.

Creating a Client SSL profile

The next step is to create an SSL profile. This profile contains the SSL certificate and Key information for offloading the SSL traffic.

To create a new Client SSL profile

1. On the Main tab, expand **Local Traffic**, click **Profiles**, and then, on the Menu bar, from the **SSL** menu, select **Client**.
2. Click the **Create** button.
3. In the **Name** box, type a name for this profile. In our example, we type **zimbra-SSL**.
4. In the Configuration section, click a check in the **Certificate** and **Key** Custom boxes.
5. From the **Certificate** list, select the name of the Certificate you imported in the *Importing keys and certificates* section.
6. From the **Key** list, select the key you imported in the *Importing keys and certificates* section.
7. Click the **Finished** button.

This completes the profile configuration.

Creating the Zimbra virtual servers

The next task is to create the virtual servers for the Zimbra roles/services that contain the load balancing pools and profiles you created.

If you are using the BIG-IP LTM to offload secure traffic (SSL/TLS), you only need virtual servers on the secure ports (such as IMAPS and POPS). If you are not using the BIG-IP LTM to offload secure traffic, you must also create virtual servers on the non-secure ports (such as IMAP and POP).

To create the virtual servers

1. On the Main tab, expand **Local Traffic**, and then click **Virtual Servers**. The Virtual Servers screen opens.
2. Click the **Create** button. The New Virtual Server screen opens.
3. In the **Name** box, type a name for this virtual server relevant to the Zimbra service (such as **zimbra-HTTPS-virtual**).
4. In the **Destination** section, select the **Host** option button.
5. In the **Address** box, type the IP address of this virtual server.
6. In the **Service Port** box, type the port associated with the Zimbra role:
   - For HTTPS, type **443**
   - For IMAPS, type **993**
   - For POPS, type **995**
   - For MTA using TLS, type **465**
   - For LDAP, type **636**

   Optional: If you are ***not*** using the BIG-IP LTM to offload SSL/TLS, you must also create the following virtual servers. Use the following Service Ports:
   - For IMAP, type **143**
   - For POP, type **110**
   - For LDAPS, type **389**
   - For MTA non-TLS, type **25**
7. In the Configuration section, select **Advanced** from the list.
8. From the **Protocol Profile (Client)** list, for the Zimbra services in the following list, select the profile you created in *Creating the WAN optimized TCP profile*, on page 16.
   - HTTPS
   - IMAPS (and IMAP if applicable)
   - MTA TLS (and non-TLS if applicable)
   - LDAP

In our example, we select **zimbra-tcp-wan**.

9. From the **Protocol Profile (Server)** list, for the Zimbra services in the following list, select the profile you created in *Creating the LAN optimized TCP profile*, on page 15:
   - HTTPS
   - IMAPS (and IMAP if applicable)
   - MTA TLS (and non-TLS if applicable)

   In our example, we select **zimbra-tcp-lan**.
10. For the HTTPS virtual server only:

    a) From the **OneConnect Profile** list, select the profile you created in *Creating the OneConnect Profile*, on page 17. In our example, we select **zimbra-HTTP**.

    b) From the **HTTP Profile** list, select the profile you created in *Creating the HTTP profile*, on page 15. In our example, we select **zimbra-HTTP**.
11. From the **SSL Profile (Client)** list, for the Zimbra services in the following list, select the name of the profile you created in *Creating a Client SSL profile*, on page 18:
    - HTTPS
    - IMAP
    - POP
    - MTS (non-TLS)
    - LDAP
12. From the **SNAT Pool** list, select **Automap**.
13. From the **Default Pool** list, select the appropriate pool you created in *Creating the pools*, on page 10 for the virtual server you are creating.
14. From the **Default Persistence Profile** list, for the virtual servers in the following list, select the profile you created in *Creating the persistence profile*, on page 16.
    - HTTPS
    - IMAPS (and IMAP if applicable)
    - POPS (and POP if applicable)
15. Click the **Repeat** button, and repeat this entire procedure for each of the Zimbra services.

This completes the BIG-IP LTM configuration.

To leave feedback on this or other F5 Solution documents, email us at ***solutionsfeedback@f5.com***.