Deployment Guide

Citrix XenDesktop

Deploying the BIG-IP LTM v11 with Citrix XenDesktop

What's inside:

Document Version
1.1

Welcome to the F5 deployment guide for Citrix® XenDesktop® with BIG-IP v11. This guide shows how to configure the BIG-IP Local Traffic Manager (LTM) for directing traffic, ensuring application availability, improving performance and providing a flexible layer of security for XenDesktop version 5.0.

Citrix XenDesktop lets you create virtualized desktops quickly and easily, then make them available to users on demand through any device.

The BIG-IP LTM provides mission critical availability, enhanced security, simple scalability and high operational resiliency to the Citrix XenDesktop deployment.

Why F5

In a Citrix XenDesktop environment, the BIG-IP LTM provides intelligent traffic management and high-availability by monitoring and managing connections to the Citrix Web Interface. In addition, the built-in performance optimization capabilities of the LTM provide faster operations to facilitate a better end-user experience. The LTM also keeps persistence records for certain connections to always be directed to the same server for a specified period of time, to ensure that the workflow in the XenDesktop environment is fully preserved.

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

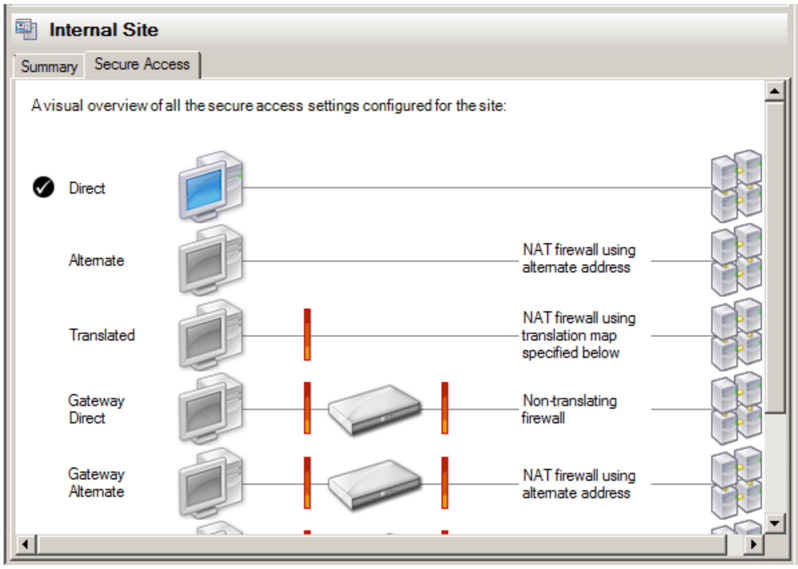
Products and versions tested

Product	Version
BIG-IP LTM	v11
Citrix XenDesktop	5.0

Prerequisites and configuration notes

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

- For this deployment guide, the Citrix XenDesktop installation must be running version 5.0.
- This document is written with the assumption that you are familiar with both F5 devices and Citrix XenDesktop products. For more information on configuring these devices, consult the appropriate documentation.
- For this deployment guide, the BIG-IP LTM system ***must*** be running version 11.0 or later. If you are using a previous version of the BIG-IP LTM system, see the Deployment Guide index on F5.com. The configuration described in this guide does not apply to previous versions.
- 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.
- *Citrix Session configuration must be set to* **Direct** *mode (see Figure 1). For specific information on configuring the Citrix Session mode, see the Citrix documentation.*


Internal Site
Summary
Secure Access

A visual overview of all the secure access settings configured for the site:

✓ Direct

Alternate
NAT firewall using alternate address
Translated
NAT firewall using translation map specified below
Gateway Direct
Non-translating firewall
Gateway Alternate
NAT firewall using alternate address

Figure 1: *Citrix Session configuration*

Configuration example

This configuration example describes the typical configuration of the BIG-IP LTM system to monitor and manage the critical component of a Citrix XenDesktop environment: the Web Interface servers (WI) and Desktop Delivery Controllers (DDC).

In this implementation, traffic to the Citrix WI and DDC servers are managed by the BIG-IP LTM system. When necessary, the BIG-IP LTM ensures that each client connects to the same member of the farm across multiple sessions using persistence. The BIG-IP LTM system is also setup to monitor the Citrix WI and DDC servers to ensure availability, authentication and to automatically mark down servers that are not operating properly.

This guide also addresses SSL offload - the ability of the BIG-IP system to terminate SSL sessions in order to offload this CPU-intensive processing from the XenDesktop WI servers. We strongly recommend SSL offload for XenDesktop deployments, which is available with a simple addition of the Client SSL profile to the WI virtual server, referred to in this guide.

If for some reason you have requirements that traffic is encrypted all the way to the XenDesktop servers, in order to preserve persistence and benefits from all F5 functionality, we recommend you terminate SSL on the BIG-IP and then re-encrypt the traffic to the Citrix server.

F5 Application Delivery Control for XenDesktop provides high availability in conjunction with advanced monitoring that looks at XenDesktop farm availability on DCC servers and authentication through WI servers provides the ultimate flexibility to deliver a resilient and available environment.

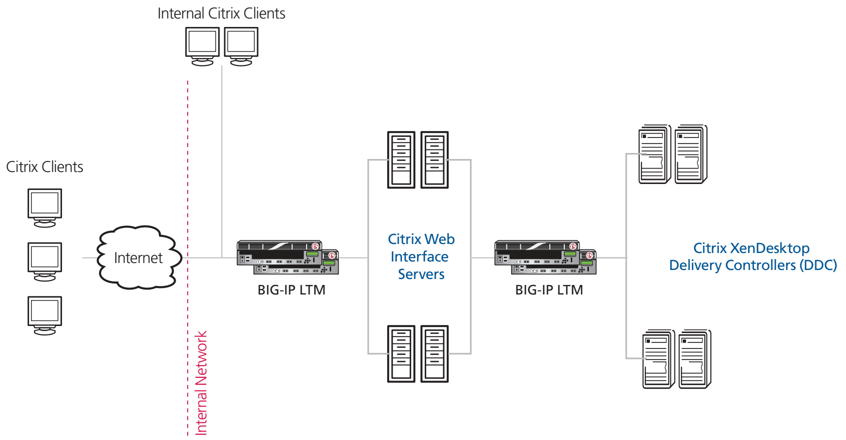


Figure 1: *Logical configuration example*

Configuring the BIG-IP LTM for Citrix XenDesktop

The following table contains a list of BIG-IP LTM configuration objects for XenDesktop 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.

Note

Use a unique name for each BIG-IP object. We recommend names that start with the application name , such as **xendesktop-wi-pool**

BIG-IP LTM Object	Non-default settings/Notes		
Health Monitor *(Main tab-->Local Traffic -->Monitors)*	See ***Health monitor configuration on page 5*** for instructions on configuring the health monitors		
Pool *(Main tab-->Local Traffic -->Pools)*	***Web Interface Pool***		
	Health Monitor	Select the Web Interface monitor you created	
	Load Balancing Method	Choose your preferred load balancing method	
	Address	Type the IP Address of the Web Interface nodes	
	Service Port	**80** (repeat Address and Service Port for all nodes)	
	Desktop Delivery Controller Pool		
	Health Monitor	Select the Desktop Delivery Controller monitor you created	
	Load Balancing Method	Choose your preferred load balancing method	
	Address	Type the IP Address of the Desktop Controller nodes	
	Service Port	**80** (repeat Address and Service Port for all nodes)	
Profiles *(Main tab-->Local Traffic -->Profiles)*	***HTTP***	Parent Profile	**http**
		Redirect Rewrite	**All**
		Insert X-Forwarded-For	**Enabled**
	HTTP Compression	Parent Profile	**wan-optimized-compression**
	Web Acceleration	Parent Profile	**optimized-caching**
	TCP WAN	Parent Profile	**tcp-wan-optimized**
	TCP LAN	Parent Profile	**tcp-lan-optimized**
	Persistence	Persistence Type	**Cookie**
	OneConnect	Parent Profile	**oneconnect**
	Client SSL	Parent Profile	**clientssl**
		Certificate and Key	Select the Certificate and key you imported
	Server SSL[1] ***(for SSL Bridging only)*** *(Profiles-->SSL)*	Parent Profile	If your Citrix server is using a certificate signed by a Certificate Authority, select **serverssl**. If your Citrix server is using a self-signed certificate, or an older SSL cipher, select **serverssl-insecure-compatible**.
		Certificate and Key	Leave the Certificate and Key set to None.
Virtual Servers *(Main tab-->Local Traffic -->Virtual Servers)*	***Web Interface HTTP virtual server***		
	Address	Type the IP Address for the virtual server	
	Service Port	**80**	
	iRule	**_sys_https_redirect**	

[1] The Server SSL profile is only necessary if you require encrypted traffic all the way to the Citrix servers. For SSL Offload (recommended), you do not need a Server SSL profile.

This table continues on the following page

BIG-IP LTM Object	Non-default settings/Notes	
Virtual Servers (*Main tab-->Local Traffic -->Virtual Servers*)	***Web Interface HTTPS virtual server***	
	Address	Type the IP Address for the virtual server
	Service Port	**443**
	Protocol Profile (client)	Select the WAN optimized TCP profile you created above
	Protocol Profile (server)	Select the LAN optimized TCP profile you created above
	OneConnect Profile	Select the OneConnect profile you created above
	HTTP Profile	Select the HTTP profile you created above
	HTTP Compression Profile	Select the HTTP compression profile you created above
	SSL Profile (Client)	Select the Client SSL profile you created above
	SSL Profile (Server)[1]	If you created a Server SSL profile only: Select the Server SSL profile you created above.
	SNAT Pool	**Automap**
	Default Pool	Select the Web Interface pool you created above
	Persistence Profile	Select the Cookie Persistence profile you created above
	Desktop Delivery Controller	
	Address	Type the IP Address for the virtual server
	Service Port	**80**
	Protocol Profile (client)	Select the WAN optimized TCP profile you created
	Protocol Profile (server)	Select the LAN optimized TCP profile you created above
	HTTP Profile	Select the HTTP profile you created above
	HTTP Compression Profile	Select the HTTP compression profile you created above
	Web Acceleration Profile	Select the Web Acceleration profile you created above
	SNAT Pool	**Automap**
	Default Pool	Select the pool you created above
	Persistence Profile	Select the Cookie Persistence profile you created above

[1] The Server SSL profile is only necessary if you created a Server SSL Profile as described in the Profiles section.

Important

After configuring the monitor as shown in the following section, be sure to also perform the procedures found in *Modifying the Citrix XenDesktop Web Interface configuration on page 8*

Health monitor configuration

To ensure traffic is directed only to those servers that are responding to requests, it is important to configure health monitors on the BIG-IP LTM to verify the availability of the servers being load balanced.

For Citrix XenDesktop, we create two advanced monitors. The first monitor is for the Web Interface servers and attempts to login to the servers by using the user name and account of a test user. We recommend you create a test user that reflects users in your environment for this purpose. If a particular server fails authentication, traffic is diverted from those servers until those devices are fixed. If all authentication is down, users will not be able to connect. We recommend setting up a Fallback Host for these situations. Please see F5 product documentation on setting up Fallback Hosts in your pools

The second monitor is for the Desktop Delivery Controller servers. This monitor determines the availability of the Desktop Farm to which users connect. If the farm is not available on the controller, it is taken out of service.

Note

The first monitor uses a user account (user name and password) that can retrieve applications from the XenDesktop server. Use an existing account for which you know the password, or create an account specifically for use with this monitor.

For the second monitor, you need to know the name of your farm. This information can be found in your Citrix XenDesktop Management Console.

Both health monitors are created using a script, available on DevCentral *https://devcentral.f5.com/wiki/TMSH.BIGIPV11-Citrix-Xen-Desktop-Monitor.ashx*.
Download the script to a location accessible by the BIG-IP device. Optionally, you can cut and paste the script directly into the TMSH editor on the BIG-IP device. However, cutting and pasting is error-prone and therefore we provide instructions here on how to copy the file to the BIG-IP device using secure-copy (SCP).

To create the Web Interface Monitor and the Desktop Delivery Controller Monitor using the script, you must first copy the script into the BIG-IP device. The following procedures show you how to copy the file both on a Windows platform using WinSCP, and on Linux, UNIX or MacOS system using SCP.

To import the script on a Windows platform using WinSCP

1. Download the script found on the following link to a computer that has access to the BIG-IP device: *https://devcentral.f5.com/wiki/TMSH.BIGIPV11-Citrix-Xen-Desktop-Monitor.ashx*
2. Open a Windows compatible SCP client. We recommend WinSCP. It is available as a free download from *http://winscp.net/*.
   The login box opens.
3. In the **Host name** box, type the host name or IP address of your BIG-IP system.
4. In the **User name** and **Password** boxes, type the appropriate administrator log on information.
5. Click **Login**. The WinSCP client opens.
6. In the left pane, navigate to the location where you saved the script in step 1.
7. In the right pane, navigate to **/shared/tmp/** (from the right pane drop-down list, select **root**, double-click **shared**, and then double-click **tmp**).
8. In the left pane, select the script and drag it to the right pane.
9. You can now safely close WinSCP.

To import the script using Linux/Unix/MacOS systems

1. Download the script:
   https://devcentral.f5.com/wiki/TMSH.BIGIPV11-Citrix-Xen-Desktop-Monitor.ashx.
2. Open a terminal session.
3. Use your built in secure copy program from the command line to copy the file. Use the following syntax:

   ```
   scp <source file> <username>@<hostname>:<Destination Directory and filename>
   ```

   In our example, the command is:

   ```
   scp create-citrix-monitor.tcl root@bigip.f5.com:/shared/tmp/create-citrix-monitor
   ```

The next task is to import the script you just copied to create the monitor. The following tasks are performed in the BIG-IP Advanced Shell (see the BIG-IP manual on how to configure users for Advanced shell access).

To run the monitor creation script

1. On the BIG-IP system, start a console session.
2. Type a user name and password, and then press Enter.
3. Change to the directory containing the creation script. In our example, we type:

   ```
   cd /shared/tmp/
   ```

   If you copied the script to a different destination, Use the appropriate directory.
4. Change the permissions on the script to allow for execute permission using the following command:

   ```
   chmod 755 create-citrix-monitor
   ```

You have now successfully imported the script. The next step is to run the script and provide the parameters to create the Citrix XenDesktop monitor for your environment.

To run the monitor script

1. At the system prompt, type tmsh and then press Enter.
   This opens the Traffic Management shell.
2. Enter CLI Script mode by typing cli script. The prompt changes to

   ```
   root@bigip-hostname(Active)(tmos.cli.script)#
   ```
3. From the command prompt, use the following command syntax, where file path is the path to the script:

   ```
   run file <file path>/<filename>
   ```

   In our example, we type

   ```
   run file /shared/tmp/create-citrix-xendesk-monitor
   ```

   The script starts, you are prompted for four arguments. You are automatically switched to interactive mode.
4. At the **What is the User Name** prompt, type the user name of the XenDesktop user.
5. At the **What is the Password** prompt, type the associated password.
6. At the **What is the Farm name** prompt, type the name of the farm of your XenDesktop farm you would like to check is available. In our example, we use **HOME**.

   Important →

   *The **Farm** name is also called the **Site** name. You can find your Farm or Site name from the XenDesktop Studio. In the navigation page, click **Configuration**. In the Site wide settings box, you see the Site name.*
7. At **What is the domain name** prompt, type the Windows domain used for authentication of users. In our example, we use **corpdomain**. Do not use the fully-qualified-domain-name from DNS here; this is referring to Windows Domain only.

The script creates the monitor. You can view the newly created monitor from the web-based Configuration utility from the Main Tab, by expanding **Local Traffic** and then clicking **Monitors**. The name of the monitors starts with the farm name you configured in step 6.

In our example, the two monitors that are created are: **Home-CitrixDDCFarm** and **Home-CitrixWICredentials**.

Modifying the Citrix XenDesktop Web Interface configuration

The next task is to make important modifications to the Citrix servers.

Modifying the Web Interface servers to point at the BIG-IP virtual server

You must modify the Web Interface server configuration so the Web Interface devices send traffic to the BIG-IP XML Broker virtual server and not directly to the Desktop Delivery Controllers. You must also make sure "Use the server list for load balancing" is unchecked, as shown below.

To modify the Web Interface servers to point at the Desktop Delivery Controller virtual server

1. From a Web Interface server, open the Access Management Console.
2. In the Navigation pane, expand **Citrix Resources, Configuration Tools, Web Interface** and then your site name.
3. From the middle column, select **Manage server farms**.
4. From the list, select the appropriate farm, and then click **Edit**.
5. In the **Server** box, select each entry and then click the **Remove** button.
6. Click the **Add** button.
7. Type the IP address of the XML Broker virtual server (the address you added in the third bullet on *page 8)*. In our example, we type **10.10.10.1**.
8. Clear the check from the **Use the server list for load balancing** box.
9. Click the **OK** button. Repeat this procedure for any/all additional Web Interface servers.
10. Repeat this change for each Web Interface server. Make sure to **restart** each Web Interface server for the changes to take effect.

Troubleshooting

This section contains troubleshooting steps in case you are having issues with the configuration.

- **Users can't connect to the Web Interface servers**
  Make sure users are trying to connect using the BIG-IP virtual server address (or a FQDN that resolves to the virtual server address).

- **Users initially see an IIS page or a page other than the Citrix log on page**
  This is typically a web server configuration issue. Make sure the proper Citrix URI is the default web site on your web server. Consult your web server documentation for more information.

  This may also be the case if all of your Web Interface servers are being marked DOWN as a result of the BIG-IP LTM health check. Check to make sure that at least one node is available. You can also use the procedure in the following section to temporarily disable the monitor itself.

- **Citrix Desktop Delivery Controller servers being incorrectly marked DOWN by the BIG-IP LTM**
  If your servers are being incorrectly marked down, you may have made an error in the configuring the health monitor script. The health monitor is very precise, calculating the Content Length header based on your responses.

  To see if the issue is coming from the health monitor, you can temporarily disable the health monitor and reattempt the connection. If the connection succeeds with the monitor disabled, we recommend you re-run the script, as the monitor is extremely difficult to manually troubleshoot.

To disable the monitor

1. From the Main tab of the BIG-IP Configuration utility, expand **Local Traffic**, and then click **Pools**.
2. From the Pool list, click the pool you created for the Desktop Delivery Controller servers.
3. In the Health Monitors section, from the **Active** list, select the health monitor and then click Remove (>>) to disable the monitor.
4. Click the **Update** button.
5. When you want to reactivate the monitor, select the Desktop Delivery Controller monitor you previously removed, click the Add (<<) button to reactivate it, and then click **Update**.

Document Revision History

Version	Description	Date
1.0	New Version	N/A
1.1	Corrected the link to the monitor script on DevCentral. Removed a reference to Appendix A for creating a Server SSL profile, and added information and instructions for using a Server SSL profile to configure SSL Bridging (SSL re-encryption).	05/07/2012

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