



Deploying the BIG-IP LTM v10 with Citrix Presentation Server 4.5

Table of Contents

Deploying the BIG-IP system v10 with Citrix Presentation Server

Prerequisites and configuration notes	1-1
Product versions and revision history	1-2
Configuration example	1-3
Configuring the BIG-IP system for Citrix Presentation Server	1-4
Running the Citrix Presentation Server application template	1-4
Modifying the TCP profiles	1-8
Configuring the Citrix Presentation Server environment for the BIG-IP System	1-9
Configuring the Citrix Web Interface	1-9
Configuring Citrix to retrieve the correct client IP address	1-9
SSL Certificates on the BIG-IP system	1-11

Manually configuring the BIG-IP LTM for Citrix Presentation Server

Creating the health monitors	2-1
Creating the pools	2-5
Creating Profiles	2-8
Creating the virtual servers	2-11
Creating a default SNAT	2-14
Configuring the Citrix Presentation Server Environment for the BIG-IP System	2-15
Configuring the Citrix Web Interface	2-15
Configuring Citrix to Retrieve the Correct Client IP address	2-15
Appendix A: Configuring the BIG-IP health monitors for Presentation Server 4.5	2-17
Defining the Citrix Web Interface health monitors	2-17
Defining the Citrix XML Broker health monitor	2-19
Configuring alternate Send and Receive strings	2-22
Optional advanced XML Broker health monitors	2-26
Appendix C: Overview of Citrix Presentation Server environment	2-28



I

Deploying the BIG-IP System v10 with Citrix Presentation Server

- Configuring the BIG-IP system for Citrix Presentation Server
- Running the Citrix Presentation Server application template
- Configuring the Citrix Presentation Server environment for the F5 BIG-IP LTM System
- SSL Certificates on the BIG-IP system

Deploying the BIG-IP system v10 with Citrix Presentation Server

Welcome to the F5 BIG-IP v10 deployment guide for Citrix® Presentation Server. This guide contains step-by-step procedures for configuring the BIG-IP Local Traffic Manager (LTM) for directing traffic, ensuring application availability, improving performance and providing a flexible layer of security for Citrix Presentation Server version 4.5.

Citrix Presentation Server provides a run-time environment for applications to be hosted on the server and accessed over the network or by using web protocols, with just keyboard strokes, mouse movements and screen updates being exchanged between the client and the server. The BIG-IP LTM provides mission critical availability, enhanced security, simple scalability and high operational resiliency to the Citrix Presentation Server deployment so that users can access resources from any device in any location as easily and securely as from within the corporate LAN.

In a Citrix Presentation Server environment, the BIG-IP LTM provides intelligent traffic management and high-availability by monitoring and managing connections to the Citrix Web Interface and the Citrix XML Broker components. 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 Presentation Server environment is fully preserved.

New in version 10.0 of the BIG-IP system are *Application Ready Templates*. These application templates ease the process of configuring the BIG-IP system. Instead of having to individually create each object that pertains to the type of application traffic you want the BIG-IP system to manage, you can run an application template. The application template automatically creates BIG-IP system objects that are customized for that application. These objects can be either local traffic objects, TMOS objects, or both.

For more information on Citrix Presentation Server, see www.citrix.com/English/ps2/products/product.asp?contentID=186

For more information on the F5 BIG-IP LTM, see www.f5.com/products/big-ip/product-modules/local-traffic-manager.html

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

Prerequisites and configuration notes

All of the procedures in this Deployment Guide are performed on the BIG-IP system. The following are prerequisites for this solution:

- ◆ For this deployment guide, the Citrix Presentation Server must be running version 4.5.
- ◆ For this deployment guide, the BIG-IP LTM system must be running version 10.0 or later. If you are using a previous version of the BIG-IP LTM system see the *Deployment Guide* index.
- ◆ If you are using the BIG-IP system to offload SSL, we assume you have already obtained an SSL certificate and key, but it is not yet installed on the BIG-IP LTM system. For more information, see *SSL Certificates on the BIG-IP system*, on page 11.
- ◆ While we strongly recommend using the application template, you can also manually configure the BIG-IP system. For more information, see *Manually configuring the BIG-IP LTM for Citrix Presentation Server*, on page 2-1.

◆ Important

All local traffic objects that an application template creates reside in administrative partition Common. Consequently, to use the application templates feature, including viewing the Templates list screen, you must have a user role assigned to your user account that allows you to view and manage objects in partition Common.

Product versions and revision history

Product and versions tested for this deployment guide:

Product Tested	Version Tested
BIG-IP System	10.0
Citrix Presentation Server	4.5

Revision history:

Document Version	Description
1.0	New deployment guide
1.1	Added a section with instructions for modifying the TCP profile settings to include an Idle Timeout value set to Indefinite. This prevents idle desktop sessions from being terminated prematurely.

Configuration example

This configuration example describes the typical configuration of the BIG-IP LTM system to monitor and manage the critical components of a Citrix Presentation Server environment, namely the Web Interface servers and the XML Broker servers.

In this implementation, traffic to the Citrix Web Interface servers and the Citrix XML Broker servers is managed by the F5 BIG-IP LTM system, and when necessary, ensures that each client connects to the same member of the farm across multiple sessions using persistence on the BIG-IP LTM. The F5 BIG-IP LTM system is also setup to monitor the Citrix Web Interface servers and Citrix XML Broker servers to ensure availability and automatically mark down servers that are not operating correctly. The ability to terminate SSL sessions in order to offload this processing from the Presentation Servers is also available with a simple addition of the Client SSL profile to the web interface virtual server referred to in this guide.

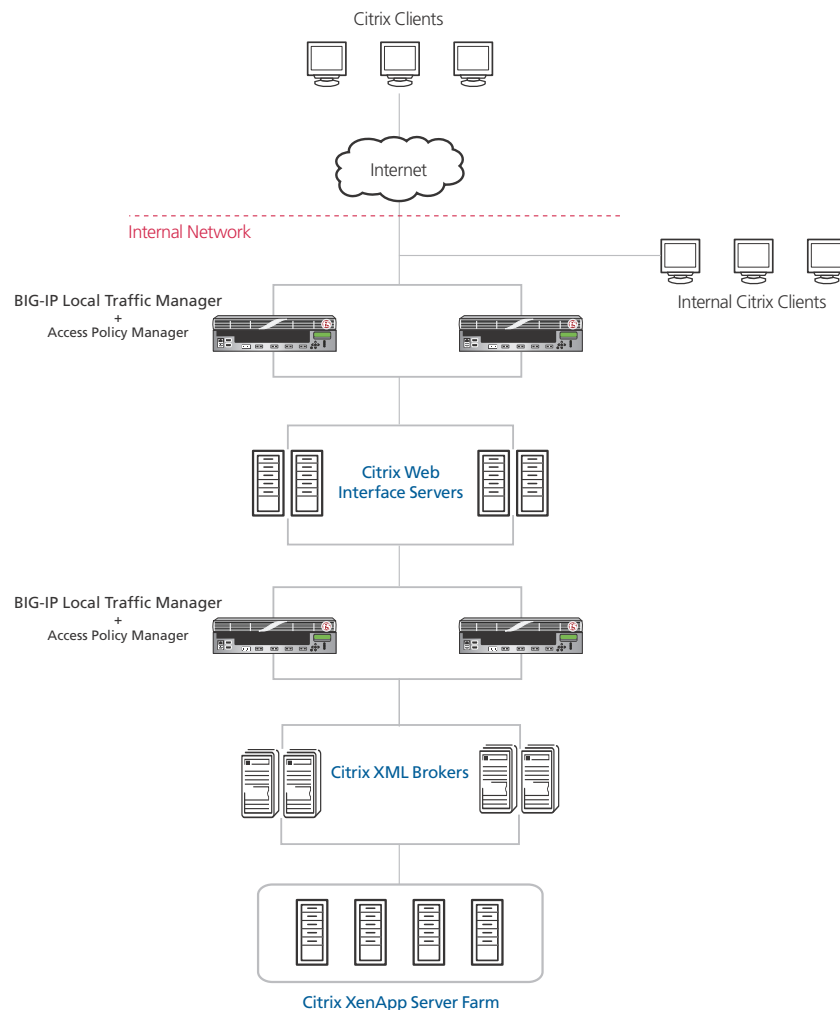


Figure 1.1 Logical configuration example

Configuring the BIG-IP system for Citrix Presentation Server

You can use the new Application Template feature on the BIG-IP system to efficiently configure a set of objects corresponding to Citrix Presentation Server. The template uses a set of wizard-like screens that query for information and then creates the required objects. At the end of the template configuration process, the system presents a list of the objects created and a description for how each object interacts with the application.

Running the Citrix Presentation Server application template

To run the Citrix Presentation Server application template, use the following procedure. For more information on specific settings, see the online help.

To run the Citrix Presentation Server application template

1. Verify that your current administrative partition is set to **Common**. The Partition list is in the upper right corner.
2. On the Main tab, expand **Templates and Wizards**, and then click **Templates**. The Templates screen opens, displaying a list of templates.
3. In the Application column, click **Citrix Presentation Server**. The Citrix Presentation Server application template opens.
4. In the **Virtual Server Questions** section, complete the following:
 - a) You can type a unique prefix for your Citrix Presentation Server objects that the template will create. In our example, we leave this setting at the default, **my_Citrix_**.
 - b) Enter the IP address for the Presentation Server *front-end Web Interface* virtual server. The system creates a virtual server named **<prefix from step a>_virtual_server**. In our example, we type **192.168.15.110**.
 - c) Enter the IP address for the Presentation Server *back-end XML Broker* virtual server. The system creates a virtual server named **<prefix from step a>_virtual_server**. In our example, we type **192.168.16.150**.
 - d) If the servers can communicate with the clients using a route through the BIG-IP system to deliver response data to the client, select **Yes** from the list. In this case, the BIG-IP does **not** translate the client's source address.

If the BIG-IP system should translate the client's source address to an address configured on the BIG-IP system, leave the list at the default setting, **No**. Selecting **No** means the BIG-IP system uses SNAT automap. See the Online Help for more information. In our example, we leave this at the default setting: **No**.

Templates and Wizards » Templates » citrix_presentation_server

Citrix Presentation Server Template

Welcome to the Citrix Presentation Server Template. This wizard creates a complete configuration optimized for managing Citrix Presentation Server traffic.

Virtual Server Questions

What unique prefix do you want the BIG-IP system to use when naming objects that this template creates?	<input type="text" value="my_Citrix_"/>
What IP Address do you want to use for the front-end Citrix Presentation Server Web Interface virtual server?	<input type="text" value="192.168.15.110"/>
What IP Address do you want to use for the back-end Citrix Presentation Server XML Broker virtual server?	<input type="text" value="192.168.16.150"/>
Do the Citrix Presentation Server servers have a route back to application clients via this BIG-IP system?	<input type="text" value="No"/>

Figure 1.2 Configuring the virtual server questions

5. In the **SSL Offload** section, complete the following
 - a) If you are not using the BIG-IP system to offload SSL from the Web Interface servers, leave this setting at the default, **No**. Continue with Step 6.

If you are using the BIG-IP system to offload SSL from the Web Interface devices, select **Yes** from the list. The SSL options appear.

- b) From the **Certificate** list, select the appropriate certificate you want to use for this deployment. If you plan to use a third party certificate, but have not yet installed it on the BIG-IP system, see *SSL Certificates on the BIG-IP system*, on page 1-11.
- c) From the **Key** list, select the appropriate key for the certificate. If you have not yet installed the key on the BIG-IP system, see *SSL Certificates on the BIG-IP system*, on page 1-11.

For information on generating certificates, or using the BIG-IP LTM 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*.

SSL Encryption Questions	
Do you want the BIG-IP system to offload SSL processing from the Citrix Presentation Server Web Interface servers?	Yes ▾
Which certificate do you want the BIG-IP system to use to authenticate the server? (You may need to import a certificate before deploying this Template.)	citrix-ssl ▾
Which key do you want the BIG-IP system to use for encryption? (You may need to import a key before deploying this Template.)	citrix-ssl ▾

Figure 1.3 Configuring the BIG-IP system for SSL Offload

6. In the **Protocol Optimization Questions** section, if most clients will be connecting to the virtual server from a WAN, select **WAN** from the list. If most clients will be connecting from a LAN, select **LAN** from the list.
This option determines the profile settings that control the behavior of a particular type of network traffic, such as HTTP connections.
7. In the **Web Interface Load Balancing Questions** section, complete the following:
 - a) From the Load Balancing Method list, select an appropriate load balancing method. In our example, we leave this setting at the default, **Least Connections (member)**.
 - b) Next, add each of the Presentation Server Web Interface devices that are a part of this deployment.
In the **Address** box, type the IP address of the first Web Interface device. In our example, we type **10.132.84.100**.
In the **Service Port** box, leave the port at **80**.
Click the **Add** button. Repeat this step for each of the Web Interface devices.
8. In the **XML Broker Load Balancing Questions** section, complete the following:
 - a) From the Load Balancing Method list, select an appropriate load balancing method. In our example, we leave this setting at the default, **Least Connections (member)**.
 - b) Next, add each of the Presentation Server XML Broker devices that are a part of this deployment.
In the **Address** box, type the IP address of the first XML Broker device. In our example, we type **10.132.94.100**.
In the **Service Port** box, leave the port at **80**.
Click the **Add** button. Repeat this step for each of the XML Broker devices.

Web Interface Load Balancing Questions

Which load balancing method do you want to use? Least Connections (member)

Address:

Service Port: Select...

Which servers do you want this virtual server to reference? (the virtual server will not be available until at least one server is added)

R:1 P:1 10.132.84.100 :80
R:1 P:1 10.132.84.101 :80
R:1 P:1 10.132.84.102 :80

XML Broker Load Balancing Questions

Which load balancing method do you want to use? Least Connections (member)

Address:

Service Port: Select...

Which servers do you want this virtual server to reference? (the virtual server will not be available until at least one server is added)

R:1 P:1 10.132.94.100 :80
R:1 P:1 10.132.94.101 :80
R:1 P:1 10.132.94.102 :80

Figure 1.4 Configuring the Load Balancing options

9. In the **Health Monitor Question** section, complete the following
 - a) Type a user account that can retrieve applications from the Presentation Server. The health monitor uses this account to verify the health of the server.
 - b) Type the password for the user account in Step a.
 - c) Type the domain associated with the user account and password from Steps a and b. In our example, we type **siterequest**.
 - d) Type the name of an application that can be returned by the Presentation Server for the user account. The health monitor will attempt to retrieve this application to verify availability. In our example, we type **Notepad** (see Figure 1.5).

10. Click the **Finished** button.

◆ Important

*For detailed information on the health monitors, see **Appendix A: Configuring the BIG-IP LTM health monitors for Presentation Server 4.5**, on page 2-17*

Health Monitor Questions	
Specify a user account that can retrieve applications from the Presentation Server.	<input type="text" value="citrixuser"/>
What is the password for the above specified user account?	<input type="password" value="....."/>
What is the domain for the above specified user account?	<input type="text" value="siterequest"/>
Specify the name of an application that can be returned by the Presentation Server for the above user. The health of the Presentation Server will be tested by attempting to retrieve this application using this user account.	<input type="text" value="Notepad"/>

Cancel Finished

Figure 1.5 Configuring the Health Monitor options

After clicking Finished, the BIG-IP system creates the relevant objects. You see a summary screen that contains a list of all the objects that were created.

Modifying the TCP profiles

Our recent testing has shown that modifying the TCP Idle Timeout value to Indefinite prevents idle desktop sessions from being terminated prematurely. Use the following procedure to modify the timeout value for both TCP profiles.

To modify the TCP profiles

1. On the Main tab, expand **Local Traffic**, and then click **Profiles**. The HTTP Profiles screen opens.
2. On the Menu bar, from the **Protocol** menu, click **tcp**.
3. From the list, select the name of the TCP LAN optimized profile created by the template. If you left the default settings, this is **my_Citrix__lan-optimized_tcp_profile**.
4. In the **Idle Timeout** row, click the **Custom** box, and then select **Indefinite** from the list.
5. Click **Update**. You return to the TCP profile list.
6. Repeat steps 3 and 4 for the WAN optimized TCP profile. If you left the default settings, this is **my_Citrix__wan-optimized_tcp_profile**.
7. Click **Update**.

This completes the modification.

Configuring the Citrix Presentation Server environment for the F5 BIG-IP LTM System

The Citrix Presentation Server environment needs to be reconfigured for integration with the F5 BIG-IP LTM system. The Citrix Web Interface is the only component within the Citrix Presentation Server environment that needs to be reconfigured for this deployment.

Configuring the Citrix Web Interface

The Web Interface servers must be reconfigured to point to the XML Broker Virtual Server address on the BIG-IP LTM. To complete the reconfiguration, you use the following procedure.

To reconfigure the Citrix Web Interface

1. Open the Citrix Access Management Console from a Web Interface server.
2. Select the Web Interface site: **Citrix Resources - Configuration Tools - Web Interface - http://**
3. From the middle column, select **Manage Server Farms**.
4. Click the appropriate server farm, and select **Edit**.
5. Select the existing entries, which should be pointing directly to the original XML Broker server addresses, and click **Remove**.
6. Click **Add**.
7. Type the IP address of the XML Broker virtual server that you entered in Step 4b of the template configuration. In our example, we type **192.168.16.150**.
8. Click **OK**.

Configuring Citrix to retrieve the correct client IP address

Citrix Presentation Server needs to be configured to look for the client IP address in the X-Forwarded-For HTTP header. Otherwise, every connection will appear to be coming from the BIG-IP LTM and not from its actual location. This can only be done by editing two Java files on each of the Web Interface servers. To complete the reconfiguration, you use the following procedure.

To reconfigure the Citrix to Read X-Forwarded-For headers for the Client IP address

1. Open the files `Inetpub\wwwroot\Citrix\AccessPlatform\app_data\auth\serverscripts\include.aspxf` and `Inetpub\wwwroot\Citrix\AccessPlatform\app_data\site\serverscripts\include.aspxf` on the Web Interface server, and find the function named `getClientAddress`.

In version 4.5, it looks like the following:

```
public string getClientAddress() {
    if ( Session[SV_AGE_CLIENT_IP] != null ) {
        return (string) Session[SV_AGE_CLIENT_IP];
    } else {
        return Request.UserHostAddress;
    }
}
```

2. Edit these functions so that they look like the following:

```
public string getClientAddress() {
    if ( Session[SV_AGE_CLIENT_IP] != null ) {
        return (string) Session[SV_AGE_CLIENT_IP];
    } else if
(Request.ServerVariables["HTTP_X_FORWARDED_FOR"] != null
) {
        return (string)
Request.ServerVariables["HTTP_X_FORWARDED_FOR"];
    } else {
        return Request.UserHostAddress;
    }
}
```

3. Repeat this for each Web Interface server.

◆ Important

Remember to restart each Web Interface server for the changes to take effect.

SSL Certificates on the BIG-IP system

Before you can enable the BIG-IP LTM system to act as an SSL proxy, you must install a SSL certificate on the virtual server that you wish to use for Citrix Presentation Server Web Interface connections on the BIG-IP LTM device. For this Deployment Guide, we assume that you already have obtained an SSL certificate, but it is not yet installed on the BIG-IP LTM system. For information on generating certificates, or using the BIG-IP LTM 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*.

Importing keys and certificates

Once you have obtained a certificate, you can import this certificate into the BIG-IP LTM system using the Configuration utility. By importing a certificate or archive into the Configuration utility, you ease the task of managing that certificate or archive. 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**. The list of existing certificates displays.
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**.

If you imported the certificate, repeat this procedure for the key.



2

Manually configuring the BIG-IP LTM System with Citrix Presentation Server

- Creating the health monitors
- Creating the pools
- Creating Profiles
- Creating the virtual servers
- Configuring the Citrix Web Interface

Manually configuring the BIG-IP LTM for Citrix Presentation Server

While we recommend using the application template, if you prefer to manually configure the BIG-IP LTM system, perform the following procedures.

Creating the health monitors

To ensure that traffic is directed 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. In this configuration, health monitors are setup for the Citrix Web Interface servers and the Citrix XML Brokers. For this deployment, we use one of F5's advanced health monitors that attempts to retrieve explicit content from the nodes. The health monitors check the nodes (IP address and port they are listening on), and based on whether correct behavior is noticed from the nodes being monitored, mark them up for the LTM to forward traffic, or mark them down so that no new requests are sent to them.

Creating the Web Interface health monitor

The first monitor we create is for the Citrix Web Interface devices. Use the following procedure. Additional information about this health monitor can be found in *Appendix A: Configuring the BIG-IP LTM health monitors for Presentation Server 4.5*, on page 2-17 for more information.

To configure the Citrix Web Interface 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 **CitrixWeb**.
4. From the **Type** list, select **HTTP**.
5. In the Configuration section, in the **Interval** and **Timeout** boxes, type an appropriate Interval and Timeout. We recommend using an Interval of **4** and a Timeout of **13**.
See the Appendix appropriate for your Presentation Server version for more information on setting these values.
6. In the **Send String** box, type a Send String specific to the application being checked. In our example, we type:
GET /Citrix/AccessPlatform
7. In the **Receive String** box, type a Receive String specific to the application being checked. In our example, we type:

Citrix

Important: See *Appendix A: Configuring the BIG-IP LTM health monitors for Presentation Server 4.5*, on page 2-17 for more information on these strings.

8. Click the **Finished** button.

The screenshot shows the 'New Monitor...' configuration window. The breadcrumb path is 'Local Traffic >> Monitors >> New Monitor...'. The 'General Properties' section contains:

- Name: CitrixWeb
- Type: HTTP
- Import Settings: http

 The 'Configuration' section is set to 'Basic' and includes:

- Interval: 4 seconds
- Timeout: 13 seconds
- Send String: GET /Citrix/AccessPlatform
- Receive String: Citrix
- User Name: (empty field)
- Password: (empty field)
- Reverse: Yes No
- Transparent: Yes No

 At the bottom are 'Update' and 'Delete' buttons.

Figure 2.1 Creating the Citrix Web Interface health monitor

Creating the Citrix WebLogon health monitor

The next step is to create a second health monitor for the Web Interface devices. We recommend first going to the additional information on this monitor found in *Defining the Citrix Web Interface health monitors*, on page 2-17.

To configure the Citrix Web Logon 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 **CitrixWebLogon**.
4. From the **Type** list, select **HTTP**. The HTTP Monitor configuration options appear.

-
- In the Configuration section, in the **Interval** and **Timeout** boxes, type an appropriate Interval and Timeout.
Because of the extended time it takes to complete the login, compared to just receiving basic web page text as the previous monitor does, we recommend a longer time period for the interval and the timeout, still maintaining the same ratio (1:3 +1).

For this application we recommend using an interval of **15** and a timeout of **46**.

- In the **Send String** box, type a Send String specific to the application being checked. In our example, we type:

```
POST /Citrix/AccessPlatform/auth/login.aspx
HTTP/1.1\r\nReferer:
http://10.133.1.127/Citrix/AccessPlatform/auth/login.aspx
\r\nContent-Type:
application/x-www-form-urlencoded\r\nContent-Length:
152\r\nConnection:
Close\r\n\r\nLoginType=Explicit&user=citrixuser&password=
Password&domain=SITEREQUEST&submitMode=submit&slLanguage=
en&ReconnectAtLoginOption=DisconnectedAndActive\r\n
```

- In the **Receive String** box, type a Receive String specific to the application being checked. In our example, we type

```
/Citrix/AccessPlatform/site/default.aspx
```

Important: See *Defining the Citrix Web Logon health monitor*, on page 18 for more information on these strings.

- Click the **Finished** button (see Figure 2.2).

Local Traffic » Monitors » New Monitor...

General Properties

Name	CitrixWebLogon
Type	HTTP
Import Settings	http

Configuration: Basic

Interval	15 seconds
Timeout	46 seconds
Send String	POST /Citrix/AccessPlatform/auth/login.aspx HTTP/1.1\r\nReferer: http://10.133.1.127/Citrix/AccessPlatform/auth/login.aspx\r\nContent-Type: application/x-www-form-urlencoded\r\nHost: 10.133.1.127\r\nContent-Length: 152\r\nConnection: Close\r\n\r\nLoginType=Explicit&user=citrixuser&password=cdfdfdfde&domain=SITEREQUEST.COM&submitMode=submit&slLanguage=eng
Receive String	/Citrix/AccessPlatform/site/default.aspx
User Name	
Password	
Reverse	<input type="radio"/> Yes <input checked="" type="radio"/> No
Transparent	<input type="radio"/> Yes <input checked="" type="radio"/> No

Update Delete

Figure 2.2 Creating the Citrix WebLogon monitor for Presentation Server 3.0

Note

For a complete explanation of the health monitor used in this section, see *Defining the Citrix Web Logon health monitor*, on page 2-18.

We recommend initially testing new monitors with at least a 1:3 +1 ratio between the Interval and the Timeout values. After the monitor functionality is verified, the values can be adjusted to obtain the best balance between rapidly determining service failure, and sufficient time to allow the monitor to complete to avoid falsely marking nodes down and adversely affecting the application being monitored.

Creating the Citrix XML Broker health monitor

The final monitor we create in this configuration is for the Citrix XML Broker devices. For more information on this monitor, see *Defining the Citrix XML Broker health monitor*, on page 2-19.

To configure the Citrix XML Broker health monitor from the Configuration utility

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 **InternalTicketTag**.
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 appropriate Interval and Timeout. For this monitor, we recommend using the default interval of **5** and the default timeout of **16**.
6. In the **Send String** box, type a Send String specific to the application being checked. In our example, we type:

```
POST /scripts/wpnbr.dll HTTP/1.1\r\nContent-Type:
text/xml\r\nHost: 10.133.40.100\r\nContent-Length:
251\r\nConnection: Close\r\n\r\n<?xml version="1.0"
encoding="UTF-8"?>\n<!DOCTYPE NFuseProtocol SYSTEM
"NFuse.dtd">\n<NFuseProtocol version="4.1">\n
<RequestAddress>\n      <Flags>no-load-bias</Flags>\n
<Name> <AppName>Notepad</AppName> </Name>
</RequestAddress>\n</NFuseProtocol>\n
```
7. In the **Receive String** box, type a Receive String specific to the application being checked. In our example, we type:
Notepad
8. Click the **Finished** button.

◆ Note

The last line of the Send String includes a variable `<AppName>` which requires the name of an actual documentation title that appears on the second screen of the application list. This example uses **notepad** for testing, but a production application should be substituted and byte size specified earlier in the send string might need to be altered as well. See *Defining the Citrix XML Broker health monitor*, on page 2-19 for additional details.

Creating the pools

The next step is to create a pool on the BIG-IP LTM system for the Citrix Web Interface servers and Citrix XML Broker servers. A BIG-IP LTM pool is a set of devices grouped together to receive traffic according to a load

balancing method. In this configuration, we create a pool for each of the major two services in the Presentation Server environment being load balanced: the Citrix Web Interface and the Citrix XML Broker.

Creating the Citrix Web Interface pool

The first pool we create is the Citrix Web Interface pool.

To create the Citrix Web Interface server pool

1. On the Main tab, expand **Local Traffic**, and then click **Pools**. The Pool screen opens.
2. In the upper right portion of the screen, click the **Create** button. The New Pool screen opens.
3. In the **Name** box, enter a name for your pool. In our example, we use **web_pool**.
4. In the Health Monitors section, select the name of the monitor you created in *Creating the Web Interface health monitor*, on page 1, and click the Add (<<) button. In our example, we select **CitrixWeb** and click the Add (<<) button, and then select the name of the monitor you created in *Creating the Citrix WebLogon health monitor*, on page 2-2. In our example, we select **CitrixWebLogon** and click the Add (<<) button again. Both monitors should now be in the **Active** list.
5. 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 (member)**.
6. For this pool, we leave the Priority Group Activation **Disabled**.
7. In the New Members section, make sure the **New Address** option button is selected.
8. In the **Address** box, type the address of the first server. In our example, we type **192.168.10.1**.
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. In our example, we repeat these steps for the remaining server in this pool, **192.168.10.2**.
12. Click the **Finished** button (see Figure 2.3).

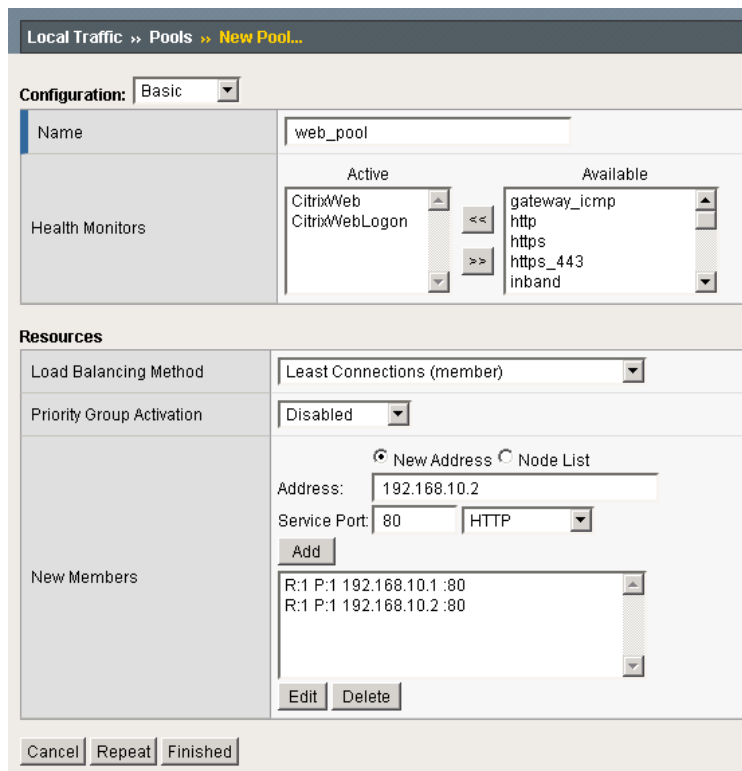


Figure 2.3 Creating the Citrix Web Interface pool

Creating the Citrix XML Broker pool

Next we create a pool for the XML Broker devices.

To create the Citrix XML Broker server pool

1. On the Main tab, expand **Local Traffic**, and then click **Pools**. The Pool screen opens.
2. In the upper right portion of the screen, click the **Create** button. The New Pool screen opens.
3. In the **Name** box, enter a name for your pool. In our example, we use **xml_pool**.
4. In the Health Monitors section, select the name of the monitor you created in *Creating the Citrix XML Broker health monitor*, on page 2-4, and click the Add (<<) button. In our example, we select **InternalTicketTag**.
5. 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 (member)**.

6. For this pool, we leave the Priority Group Activation **Disabled**.
7. In the New Members section, make sure the **New Address** option button is selected.
8. In the **Address** box, type the address of the first XML Broker device. In our example, we type **192.168.20.1**.
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. In our example, we repeat these steps three times for the remaining servers in this pool, **192.168.20.2-4**.
12. Click the **Finished** button.

Creating Profiles

The BIG-IP system uses profiles for greater control over managing network traffic while making network traffic management easy and efficient. A profile is an object that contains user-configurable settings, with default values, for controlling the behavior of a particular type of network traffic, such as HTTP connections.

Although it is possible to use the default profiles, we strongly recommend that you create new profiles based on the default parent profiles. Creating new profiles allows you to easily modify the profile settings specific to your deployment, and ensures that you do not accidentally overwrite the default profile. We also recommend however, that you use the default settings in the cookie persistence profile for this configuration (Insert method, Session based).

Creating an HTTP profile

The first new profile we create is an HTTP profile. The HTTP profile contains numerous configuration options for how the BIG-IP LTM system handles HTTP traffic. Our testing with Citrix Presentation Server shows that while we see a great deal of benefit from compression, caching only produces a minimal improvement. Therefore, we recommend using the **http-wan-optimized-compression** parent profile. This profile uses specific compression (among other) settings to optimize traffic over the WAN.

Citrix Presentation Server must have access to the IP address of the connecting clients in order to be fully functional. Some of the BIG-IP LTM features used in this Deployment Guide obscure this information. To overcome this, we use the following HTTP profile to insert an **X-Forwarded-For** header into the HTTP header. This supplies the IP address of the client so it is available to Citrix Presentation Server.

To create a new HTTP profile

1. On the Main tab, expand **Local Traffic**, and then click **Profiles**. The HTTP Profiles screen opens.
2. In the upper right portion of the screen, click the **Create** button.
3. In the **Name** box, type a name for this profile. In our example, we type **citrix-http-opt**.
4. From the **Parent Profile** list, select **http-wan-optimized-compression**.
5. From the Insert **XForward For** row, click the Custom box, and then select **Enabled** from the list.
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.

Creating the TCP profiles

The next profiles we create are the TCP profiles. If most of the Citrix Presentation Server users are accessing the devices via a Local Area Network, we recommend using the **tcp-lan-optimized** (for server-side TCP connections) parent profile. If the majority of the users are accessing the system from remote or home offices, we recommend using an additional TCP profile, called **tcp-wan-optimized** (for client side TCP connections). The use of these optimized profiles is optional, you can alternatively use the base TCP parent profile if appropriate for your configuration.

For the TCP profiles, we set the Idle Timeout value to Indefinite to prevent idle desktop sessions from being terminated prematurely.

Creating the LAN optimized TCP profile

First we configure the LAN optimized profile. If you do not want to use this optimized profile, you can choose the default TCP parent profile.

To create a new TCP 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 **Protocol** menu, click **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 **citrix-tcp-lan**.
5. From the **Parent Profile** list, select **tcp-lan-optimized**.
6. In the **Idle Timeout** row, click the **Custom** box, and then select **Indefinite** from the list.
7. Modify any of the other settings as applicable for your network. In our example, we leave the settings at their default levels.

8. Click the **Finished** button.

Creating the WAN optimized TCP profile

Now we configure the WAN optimized profile. Remember, if most of the users are accessing the system over the LAN or other low latency links, you do not need to create this profile.

To create a new TCP WAN optimized 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 **Protocol** menu, click **tcp**.
3. In the upper right portion of the screen, 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 **citrix-tcp-wan**.
5. From the **Parent Profile** list, select **tcp-wan-optimized**.
6. In the **Idle Timeout** row, click the **Custom** box, and then select **Indefinite** from the list.
7. Modify any of the other settings as applicable for your network. In our example, we leave the settings at their default levels.
8. Click the **Finished** button.

Creating the persistence profile

The next profile we create is a Persistence profile. We recommend using persistence for Citrix devices, although the type of persistence depends on your configuration. In our example, use cookie persistence (HTTP cookie insert).

To create a new cookie persistence profile

1. On the Main tab, expand **Local Traffic**, and then click **Profiles**. The HTTP Profiles screen opens.
2. On the Menu bar, click **Persistence**. The Persistence Profiles screen opens.
3. In the upper right portion of the screen, click the **Create** button. The New Persistence Profile screen opens.
4. In the **Name** box, type a name for this profile. In our example, we type **citrix-cookie**.
5. From the **Persistence Type** list, select **Cookie**. The configuration options for cookie persistence appear.
6. Modify any of the settings as applicable for your network. In our example, we leave the settings at their default levels.

-
7. Click the **Finished** button.

Creating the virtual servers

A virtual server with its virtual IP address is the visible, routable entity through which the servers in a load balancing pool are made available to the client (the IP address to give clients or add to DNS).

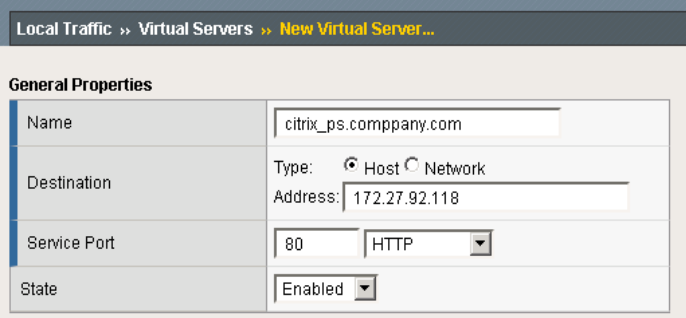
The next step in the configuration is to configure a virtual server that references the pools and profiles created in the preceding sections.

Creating the Citrix Web Interface virtual server

The first virtual server we create is for the Citrix Web Interface servers.

To create the Citrix Web Interface virtual server

1. On the Main tab, expand **Local Traffic**, and then click **Virtual Servers**. The Virtual Servers screen opens.
2. In the upper right portion of the screen, click the **Create** button. The New Virtual Server screen opens.
3. In the **Name** box, type a name for this virtual server. In our example, we type **citrix_ps.company.com**.
4. In the **Destination** section, select the **Host** option button.
5. In the **Address** box, type the IP address of this virtual server. In our example, we use **172.27.92.118**.
6. In the **Service Port** box, type **80**, or select **HTTP** from the list.



General Properties	
Name	citrix_ps.comppany.com
Destination	Type: <input checked="" type="radio"/> Host <input type="radio"/> Network
	Address: 172.27.92.118
Service Port	80 HTTP
State	Enabled

Figure 2.4 Creating the Citrix virtual server

7. From the Configuration list, select **Advanced**. The Advanced configuration options appear.
8. Leave the **Type** list at the default setting: **Standard**.

9. From the **Protocol Profile (Client)** list select the name of the profile you created in the *Creating the WAN optimized TCP profile* section. If you did not create a WAN optimized profile, select the LAN optimized profile as in the following Step. In our example, we select **citrix-tcp-wan**.
10. From the **Protocol Profile (Server)** list, select the name of the profile you created in the *Creating the LAN optimized TCP profile* section. In our example, we select **citrix-tcp-lan**.
11. From the HTTP Profile list, select the name of the profile you created in the *Creating an HTTP profile* section. In our example, we select **citrix-http-opt**.

Configuration: Advanced	
Type	Standard
Protocol	TCP
Protocol Profile (Client)	citrix-tcp-wan
Protocol Profile (Server)	citrix-tcp-lan
OneConnect Profile	None
NTLM Conn Pool	None
HTTP Profile	citrix-http-opt
FTP Profile	None
SSL Profile (Client)	None
SSL Profile (Server)	None
Authentication Profiles	<div style="display: flex; justify-content: space-between;"> <div>Enabled</div> <div>Available</div> </div> <div style="display: flex; justify-content: space-between; margin-top: 5px;"> <div style="border: 1px solid gray; padding: 2px;"><<</div> <div style="border: 1px solid gray; padding: 2px;">ssl_cc_ldap</div> </div>

Figure 2.5 Selecting the Citrix profiles for the virtual server

12. In the Resources section, from the **Default Pool** list, select the pool you created in *Creating the Citrix Web Interface pool*, on page 2-6. In our example, we select **web_pool**.
13. From the **Default Persistence Profile** list, select the persistence profile you created in the *Creating the persistence profile* section. In our example, we select **citrix-cookie**.
14. Click the **Finished** button (see Figure 2.6).

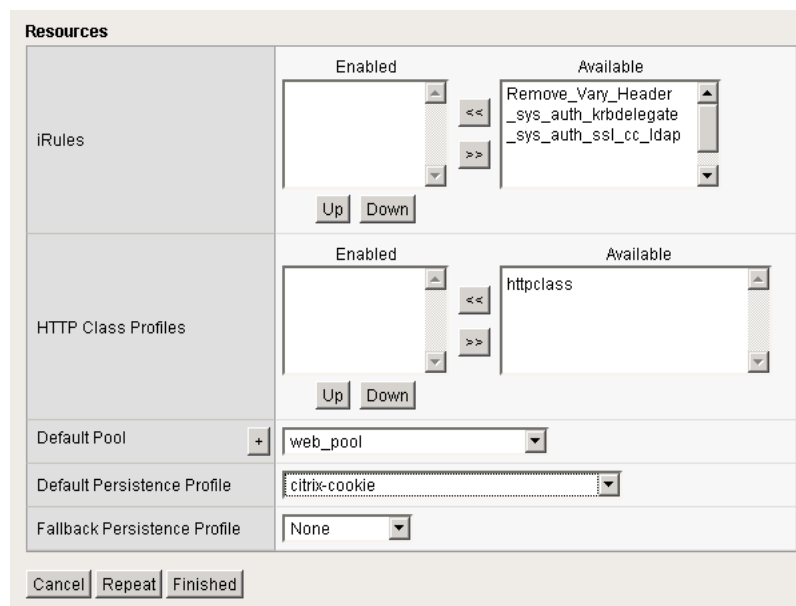


Figure 2.6 Adding the Pool and Persistence profile to the virtual server

Creating the Citrix XML Broker virtual server

Next we create a virtual server for the Citrix XML Broker servers.

To create the Citrix XML Broker virtual server

1. On the Main tab, expand **Local Traffic**, and then click **Virtual Servers**. The Virtual Servers screen opens.
2. In the upper right portion of the screen, click the **Create** button. The New Virtual Server screen opens.
3. In the **Name** box, type a name for this virtual server. In our example, we type **citrix.xml.site.com**.
4. In the **Destination** section, select the **Host** option button.
5. In the **Address** box, type the IP address of this virtual server. In our example, we use **192.168.20.100**.
6. In the **Service Port** box, type **80**, or select **HTTP** from the list.
7. From the Configuration list, select **Advanced**. The Advanced configuration options appear.
8. Leave the **Type** list at the default setting: **Standard**.
9. From the **Protocol Profile (Client)** list select the name of the profile you created in the *Creating the WAN optimized TCP profile* section. If you did not create a WAN optimized profile, select the LAN optimized profile as in the following Step. In our example, we select **citrix-tcp-wan**.

10. From the **Protocol Profile (Server)** list, select the name of the profile you created in the *Creating the LAN optimized TCP profile* section. In our example, we select **citrix-tcp-lan**.
11. From the HTTP Profile list, select the name of the profile you created in the *Creating an HTTP profile* section. In our example, we select **citrix-http-opt**.
12. In the Resources section, from the **Default Pool** list, select the pool you created in *Creating the Citrix Web Interface pool*, on page 6. In our example, we select **xml_pool**.
13. From the **Default Persistence Profile** list, select the persistence profile you created in the *Creating the persistence profile* section. In our example, we select **citrix-cookie**.
14. Click the **Finished** button.

Creating a default SNAT

A secure network address translation (SNAT) ensures the proper routing of connections between the Web Interface servers to the XML Broker servers. For the configuration described in this deployment guide, we configure a default SNAT. While not every network topology requires a default SNAT, if the Web Interface and XML Broker are on the same subnet, a default SNAT is mandatory.

For more information on SNATs, see the BIG-IP LTM documentation.

◆ Note

If you do not want source address translation on client connections from the external VLAN, you can disable the default SNAT for the external VLAN.

To create a default SNAT

1. On the Main tab, expand **Local Traffic**, and then click **SNATs**. The SNATs screen opens.
2. In the upper right portion of the screen, click the **Create** button. The New SNAT screen opens.
3. In the **Name** box, type a name for this SNAT. In our example, we type **DefaultSNAT**.
4. In the **Translation** list, select **Automap**.
5. **Optional:** If you to disable (or enable) the default SNAT for specific VLANs, from the VLAN Traffic list, select either **Enabled on** or **Disabled on** from the list. From the Available list, select the appropriate VLAN and click the Add (<<) button to move it to the Selected list.
6. Click the **Finished** button.

Configuring the Citrix Presentation Server Environment for the F5 BIG-IP LTM System

The Citrix Presentation Server environment needs to be reconfigured for integration with the F5 BIG-IP LTM system. The Citrix Web Interface is the only component within the Citrix Presentation Server environment that needs to be reconfigured for this deployment.

Configuring the Citrix Web Interface

The Web Interface servers must be reconfigured to point to the XML Broker Virtual Server address on the BIG-IP LTM. To complete the reconfiguration, you use the following procedure.

To reconfigure the Citrix Web Interface

1. Open the Citrix Access Management Console from a Web Interface server.
2. Select the Web Interface site: **Citrix Resources - Configuration Tools - Web Interface - http://**
3. From the middle column, select **Manage Server Farms**.
4. Click the appropriate server farm, and select **Edit**.
5. Select the existing entries, which should be pointing directly to the original XML Broker server addresses, and click **Remove**.
6. Click **Add**.
7. Type the XML Broker's Virtual Server address that you configured in *Creating the Citrix XML Broker virtual server*, on page 13. In our example, we type **192.168.20.100**.
8. Click **OK**.

Configuring Citrix to Retrieve the Correct Client IP address

Citrix Presentation Server needs to be configured to look for the client IP address in the X-Forwarded-For HTTP header. Otherwise, every connection will appear to be coming from the BIG-IP LTM and not from its actual location. This can only be done by editing two Java files on each of the Web Interface servers. To complete the reconfiguration, you use the following procedure.

To reconfigure the Citrix to Read X-Forwarded-For headers for the Client IP address

1. Open the files `Inetpub\wwwroot\Citrix\AccessPlatform\app_data\auth\serverscripts\include.aspxf` and `Inetpub\wwwroot\Citrix\AccessPlatform\app_data\site\serverscripts\include.aspxf` on the Web Interface server, and find the function named `getClientAddress`.

In version 4.5, it looks like the following:

```
public string getClientAddress() {  
    if ( Session[SV_AGE_CLIENT_IP] != null ) {  
        return (string) Session[SV_AGE_CLIENT_IP];  
    } else {  
        return Request.UserHostAddress;  
    }  
}
```

2. Edit these functions so that they look like the following:

```
public string getClientAddress() {  
    if ( Session[SV_AGE_CLIENT_IP] != null ) {  
        return (string) Session[SV_AGE_CLIENT_IP];  
    } else if  
(Request.ServerVariables["HTTP_X_FORWARDED_FOR"] != null  
) {  
        return (string)  
Request.ServerVariables["HTTP_X_FORWARDED_FOR"];  
    } else {  
        return Request.UserHostAddress;  
    }  
}
```

3. Repeat this for each Web Interface server.

Important

Remember to restart each Web Interface server for the changes to take effect.

Appendix A: Configuring the BIG-IP LTM health monitors for Presentation Server 4.5

This Appendix contains a detailed explanation of the BIG-IP LTM health monitors used for Citrix Presentation Server 4.5.

Defining the Citrix Web Interface health monitors

In the configuration example used in this guide, two custom HTTP Extended Content Verification (ECV) monitors were used to monitor the health of the Citrix Web Interface - CitrixWeb and Citrix WebLogon.

A HTTP ECV monitor is used to check the status of Hypertext Transfer Protocol (HTTP) traffic. The HTTP ECV monitor attempts to open a connection to the server on port 80, and uses the HTTP protocol to send and receive content. The check is successful when the content matches the Receive String value.

Defining the Web Interface health monitor

When a user tries to access the Web Interface server from a web browser, the first page received is usually the Web Interface welcome page, which includes the login form. The Web Interface prevents access to any of the site's other main scripts directly prior to authentication and includes a built-in URL filter that directs the user to the login page on such access.

If the web server hosting the Web Interface server is operational and if the Web Interface server is running, a simple request to the IP address of the server should result in a response with a valid welcome page consisting of the login fields. By default, the first page at which all users start is **/auth/login.aspx** for Web Interface version 4.x. This is also the page that the users are redirected to if authentication fails.

For this monitor, we send a simple GET request to the Web Interface server (**GET / Citrix/AccessPlatform**) for the default page of the site and expect to see the string **Citrix** embedded in the content. The check passes if the response from the Web Interface server returns the valid string. This helps us determine that both the web server and the Web Interface server are responding and operational.

The following is the Send String in our example:

```
GET /Citrix/AccessPlatform
```

Figure 2.7 Example Send String for the Web Interface monitor

Defining the Citrix Web Logon health monitor

The Web Interface server first authenticates a user before displaying the list of published applications that the user can access. The Citrix Web Interface can be configured for explicit authentication, single sign-on, smart card authentication or anonymous authentication. For the purposes of this deployment guide and the configuration example, we are assuming that the Citrix Web Interface is configured for Explicit Authentication.

When a user accesses the Web Interface server from a web browser, the Web Interface generates a web login form requiring valid User Name, Password and Domain values. When the user clicks on the Log In button, the credentials entered in the login form are sent to the Web Interface server using HTTP or HTTPS (depending on the Web Interface server configuration). The Web Interface server translates the user credentials received from the HTTP POST request into XML, and forwards them on to the XML Broker as part of the application retrieval request. The XML Broker validates the credentials and responds to the Web Interface with the list of applications that the user has access to. A sample user login request to a Web Interface server is shown below.

```
POST /Citrix/MetaFrame/default/login.aspx HTTP/1.1
Content-Type: application/x-www-form-urlencoded
User-Agent: Mozilla/5.0 (Windows; U; Windows NT 5.1; en-US;
rv:1.8.1.6) Gecko/20070725 Firefox/2.0.0.6
state=LOGIN&LoginType=Explicit&user=user1&password=password1&do
main=domain1&login=Log+In
```

If the Web Interface server is operational and accepting requests, a successful logon event to the Web Interface will result in a response with a list of applications available to the user and content such as the application icons and application launch files. By default, the Web Interface will direct the authenticated user to **/site/default.aspx** immediately after a successful logon attempt. Moreover, the web page received by an authenticated user response includes the contents of the file **/site/footer.txt** within the page.

For this monitor, we send a POST request to the Web Interface server with the credentials of a valid user in the Citrix Presentation Server environment. The POST request sent to the Web Interface server closely mimics a real web browser request to ensure that it is accepted by the server and to ensure the receipt of a valid response that indicates a functional server. A valid response if the user authentication is successful would include the string **/Citrix/AccessPlatform/site/default.aspx** embedded in the content. The check passes if the response from the Web Interface server has the valid string. This helps us determine that the Web Interface server is responding, fully functional and accepting requests.

The following is the complete Send String in our example:

```
POST /Citrix/AccessPlatform/auth/login.aspx
HTTP/1.1\r\nReferer:
http://10.133.40.50/Citrix/AccessPlatform/auth/login.aspx\r\n
Content-Type:
application/x-www-form-urlencoded\r\nContent-Length:
136\r\nConnection:
Close\r\n\r\nLoginType=Explicit&user=ul&password=Password&dom
ain=CITRIX&submitMode=submit&slLanguage=en&ReconnectAtLoginOp
tion=DisconnectedAndActive\r\n
```

Figure 2.8 Example Send String for the Web Logon monitor

◆ Important

Variables in red text must be replaced with a valid IP address, user name, password or domain. The IP Address should be set to the DNS name or the IP address of the Virtual Server.

*In addition, the Content Length value must be replaced with the new total length of the string beginning with **LoginType=Explicit** and ending with **DisconnectedAndActive**. This value changes depending on the length of the actual user name, password and domain values used. A count of the characters, minus a count of any escape (\) characters, is all that is required to determine the Content Length.*

◆ Note

*Text of the Send String entry used in this section can be cut and paste into the **Send String** field in the BIG-IP LTM GUI health monitor page to speed the development of monitors for the Citrix Presentation Server application. Text of the Receive String entry in the configuration section can be cut & paste into the **Receive String** field in the BIG-IP LTM GUI on the health monitor page, when using the corresponding Send String. The script text here can be used as a guideline for how a Send String or Receive String should be built.*

All script text is subject to change depending on many factors including application version, application developer, changes in content, application alterations, system or network design changes, and other factors.

Defining the Citrix XML Broker health monitor

This Appendix contains a detailed explanation of the Citrix XML Broker health monitor used in this guide. In the configuration example used in this guide, a custom HTTP Extended Content Verification (ECV) monitor was used to monitor the health of the XML Brokers and the Citrix Presentation Server farm - InternalTicketTag.

When an authenticated user clicks on an application icon from the web page displaying the list of applications the user can access, a request to launch the application is sent to the Web Interface server. The Web Interface server queries the XML Broker for the address of the least busy Presentation Server that hosts the application that the user is requesting. Once the target server is identified and checked to ensure that it is responding, the XML Broker responds to the Web Interface server with the IP Address of the server. A proper response from the XML Broker results in the Web Interface server responding to the user with a **launch.ica** file for the requested application. The **launch.ica** file is executed and the user initiates an ICA connection to access the application on the target Presentation Server.

When the user clicks an application icon, the Web Interface server sends a request, similar to the following example, to the XML Broker server. In this example, a request for the application Notepad is generated.

```
POST /scripts/wpnbr.dll HTTP/1.1
Content-Type: text/xml
<?xml version="1.0" encoding="UTF-8"?>
<!DOCTYPE NFuseProtocol SYSTEM "NFuse.dtd">
<NFuseProtocol version="4.1">
  <RequestAddress>
    <Flags>no-load-bias</Flags>
    <Name>
      <AppName>notepad</AppName>
    </Name>
  </RequestAddress>
</NFuseProtocol>
```

Once the target server has been identified, the XML Broker responds to the Web Interface request with the IP address, with a response similar to the following example:

```
HTTP/1.1 200 OK
Content-type: text/xml
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE NFuseProtocol SYSTEM "NFuse.dtd">
<NFuseProtocol version="4.1">
  <ResponseAddress>
    <ServerAddress addressType="dot">5.214.10.251</ServerAddress>
    <ServerType>win32</ServerType>
    <ConnectionType>tcp</ConnectionType>
    <ClientType>ica30</ClientType>
    <TicketTag>IMAHostId:13093</TicketTag>
    <FarmLoadHint>0</FarmLoadHint>
  </ResponseAddress>
</NFuseProtocol>
```

When the IP Address of the least busy target server for a published application cannot be determined, the Web Interface server requests results in a response with errors and does not include the <TicketTag> entries. This error condition can occur for any number of reasons, such as if the XML Service on the XML Broker is not functioning correctly, if there are problems with the IMA service on the target server or the XML Broker, if logons are disable on the target server, or if the Local Host Cache on the XML Broker is invalid, and so on. A sample response with the error condition where the XML Broker could not find a result to the Web Interface query is shown in the following example:

```
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE NFuseProtocol SYSTEM "NFuse.dtd">
<NFuseProtocol version="4.1">
  <ResponseAddress>
    <ErrorId>unspecified</ErrorId>
    <MPSError type="IMA">0x80000024</MPSError>
    <BrowserError>0x00000024</BrowserError>
  </ResponseAddress>
</NFuseProtocol>
```

If the XML Broker server is functioning correctly and the Presentation Server farm is operational and accepting requests for applications hosted on the farm, and if there is at least one Presentation Server available with the requested application, a successful query from the Web Interface server will result in a response with <TicketTag> entry embedded in the content.

For this monitor, the BIG-IP LTM sends a POST request to the XML Broker server for the IP Address of a target server hosting the Notepad application. The POST request sent to the XML Broker server closely mimics a real XML request that a Web Interface server would send to ensure that it is accepted by the XML Broker server and for the receipt of a valid response. If the request is successful, the XML response sent by the XML Broker server would include the string **TicketTag** embedded in content. The check passes if the response from the XML Broker server has the valid string. This helps determine that the XML Broker server is operational and that the Presentation Server farm is fully functional and accepting application requests.

The following is the code for the Send String in our monitor:

```
POST /scripts/wpnbr.dll HTTP/1.1\r\nContent-Type:
text/xml\r\nHost: 10.133.40.100\r\nContent-Length:
251\r\nConnection: Close\r\n\r\n<?xml version="1.0"
encoding="UTF-8"?\>\n<!DOCTYPE NFuseProtocol SYSTEM
"NFuse.dtd"\>\n<NFuseProtocol version="4.1"\>\n
<RequestAddress>\n      <Flags>no-load-bias</Flags>\n      <Name>
<AppName>Notepad</AppName> </Name>
</RequestAddress>\n</NFuseProtocol>\n
```

Figure 2.9 Example Send String for the XML Broker monitor

◆ Important

Variables in red text must be replaced with a valid IP address and an application name that is actually hosted on the Presentation Server farm. The IP Address should be set to the DNS name or the IP address of the Virtual Server.

In addition, the Content Length value must be replaced with the new total length of the string beginning with `<?xml version="1.0">` and ending with `</NFuseProtocol>`. This value changes depending on the length of the actual user name, password and domain values used. A count of the characters, minus a count of any escape (\) characters, is all that is required to determine the Content Length.

◆ Note

Text of the Send String used in this section can be cut & paste into the **Send String** field in the BIG-IP LTM GUI health monitor page to speed the development of monitors for the Citrix Presentation Server application (v3.0 and v4.5). Text of the Receive String from the configuration section, can be cut & paste into the **Receive String** field in the BIG-IP LTM GUI on the health monitor page, when using the corresponding Send String. The script text here can be used as a guideline for how a Send String or Receive String should be built.

All script text is subject to change depending on many factors including application version, application developer, changes in content, application alterations, system or network design changes, and other factors.

Configuring alternate Send and Receive strings

Another good candidate for a health monitor Send string is one that performs application enumeration. This is the method by which the Web Interface asks the XML Broker to enumerate which applications are available. The resultant information is used to populate the list of applications that the user may select.

```
POST /scripts/wpnbr.dll
HTTP/1.1
Content-Type: text/xml
Host: 10.133.40.100
Content-Length: 310
Connection: Close
<?xml version="1.0" encoding="UTF-8"?>
<!DOCTYPE NFuseProtocol SYSTEM "NFuse.dtd">
<NFuseProtocol version="4.6">
  <RequestAppData>
    <DesiredDetails>defaults</DesiredDetails>
    <ServerType>all</ServerType>
    <ClientType>ica30</ClientType>
    <ClientType>content</ClientType>
  </RequestAppData>
</NFuseProtocol>
```

The XML Broker responds back with the following:

```
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE NFuseProtocol SYSTEM "NFuse.dtd">
<NFuseProtocol version="4.6">
  <ResponseAppData>
    <AppDataSet>
      <Scope traverse="onelevel"/>
      <AppData>
        <InName>Notepad</InName>
        <FName>Notepad</FName>
        <Details>
          <Settings appisdisabled="false"
appisdesktop="false">
            <Folder/>
            <Description>notepad</Description>
            <WinWidth>1024</WinWidth>
            <WinHeight>768</WinHeight>
            <WinColor>8</WinColor>
            <WinType>pixels</WinType>
            <WinScale>1</WinScale>
            <SoundType minimum="false">basic</SoundType>
            <VideoType minimum="false">none</VideoType>
            <Encryption minimum="false">basic</Encryption>
            <AppOnDesktop value="false"/>
            <AppInStartmenu value="false"/>
            <PublisherName>Farm2</PublisherName>
```

```

        <SSEnabled>>false</SSEnabled>
        <RemoteAccessEnabled>>false</RemoteAccessEnabled>
    </Settings>
</Details>
<SeqNo>1206119789</SeqNo>
<ServerType>win32</ServerType>
<ClientType>ica30</ClientType>
</AppData>
<AppData>
    <InName>Wireshark</InName>
    <FName>Wireshark</FName>
    <Details>
        <Settings appisdisabled="false"
        appisdesktop="false">
            <Folder/>
            <Description/>
            <WinWidth>1024</WinWidth>
            <WinHeight>768</WinHeight>
            <WinColor>8</WinColor>
            <WinType>pixels</WinType>
            <WinScale>1</WinScale>
            <SoundType minimum="false">basic</SoundType>
            <VideoType minimum="false">none</VideoType>
            <Encryption minimum="false">basic</Encryption>
            <AppOnDesktop value="false"/>
            <AppInStartmenu value="false"/>
            <PublisherName>Farm2</PublisherName>
            <SSEnabled>>false</SSEnabled>
            <RemoteAccessEnabled>>false</RemoteAccessEnabled>
        </Settings>
    </Details>
    <SeqNo>1206048557</SeqNo>
    <ServerType>win32</ServerType>
    <ClientType>ica30</ClientType>
</AppData>
</AppDataSet>
</ResponseAppData>
</NFuseProtocol>

```

If the XML Broker is healthy, there should be an **<AppData>** section for each application available. As a result, it is easy to ensure that it is working by setting the Receive string to look for the name of one of your available applications. In our case, we chose **Notepad**.

The following is the code for the Send String in our monitor:

```
POST /scripts/wpnbr.dll HTTP/1.1\r\nContent-Type:  
text/xml\r\nHost: 10.133.40.100\r\nContent-Length:  
310\r\nConnection: Close\r\n\r\n<?xml version="1.0"  
encoding="UTF-8" ?>\n<!DOCTYPE NFuseProtocol SYSTEM  
\nNFuse.dtd\n>\n<NFuseProtocol version="4.6" >\n  <RequestAppData>\n    <DesiredDetails>defaults</DesiredDetails>\n    <ServerType>all</ServerType>\n    <ClientType>ica30</ClientType>\n    <ClientType>content</ClientType>\n  </RequestAppData>\n</NFuseProtocol>
```

Figure 2.10 Send string for the alternate XML Broker monitor

In our example, the Receive string is simply **Notepad**.

◆ Important

Variables in red text must be replaced with a valid IP address and an application name that is actually hosted on the Presentation Server farm. The IP Address can be set to any Host name or IP Address that the XML Broker server will accept. The DNS name for the Web Interface Virtual Server is commonly used here. This may require unique monitors for each node if there is not a suitable universal value for the pool. In addition, the Content Length value must be replaced with the new total length of the string beginning with `<?xml version="1.0"` and ending with `</NFuseProtocol>`. This value changes depending on the length of the actual user name, password and domain values used. A count of the characters, minus a count of any escape (\) characters, is all that is required to determine the Content Length.

◆ Note

Text of the Send String used in this section can be cut & paste into the **Send String** field in the BIG-IP LTM GUI health monitor page to speed the development of monitors for the Citrix Presentation Server application (v3.0 and v4.5). Text of the **Receive String** from the configuration section, can be cut and paste into the Receive String field in the BIG-IP LTM GUI on the health monitor page, when using the corresponding Send String. The script text here can be used as a guideline for how a Send String or Receive String should be built.

All script text is subject to change depending on many factors including application version, application developer, changes in content, application alterations, system or network design changes, and other factors.

Optional advanced XML Broker health monitors

The following two optional health monitors check the XML Broker's ability to validate credentials. This is already partially checked by the web interface login monitor. However, if a login problem is with a particular XML Broker and not with the web interface server, the BIG-IP LTM could mark the web interface server down but leave the broken XML Broker up. These two monitors mark the XML Broker as down instead of the Web Interface.

Both of the following monitors are reverse monitors. A reverse monitor is one in which the receive string is something we expect not to see in a normal case. The servers will be marked down if this string is seen.

Review the following optional monitors and, if applicable, choose the one best suited for your configuration.

XML Broker Credential Validation Health Monitor I

The first health monitor sends a **RequestValidateCredentials** request with dummy user credentials to the XML Broker. We expect to see a credentials-failed error message. However, should the XML Broker lose its connection to its domain controller and thus lose the ability to validate users credentials, a different error message is reported.

This monitor is configured as a reverse monitor. We check that the receive string, `<MPSError type="IMA">0x80130007</MPSError>`, is not returned.

The following is the code for the Send String in this monitor:

```
POST /scripts/wpnbr.dll HTTP/1.1\r\nContent-Type:
text/xml\r\nHost: 10.133.40.100\r\nContent-Length:
329\r\n\r\n<?xml version="1.0"
encoding="UTF-8"?\>\n<!DOCTYPE NFuseProtocol SYSTEM
"NFuse.dtd"\>\n<NFuseProtocol version="4.6"\>\n
<RequestValidateCredentials>\n <Credentials>\n
<UserName>user</UserName>\n <Password
encoding="cleartext">Password</Password>\n
<Domain>citrix</Domain>\n </Credentials>\n
</RequestValidateCredentials>\n</NFuseProtocol>\n
```

Figure 2.11 Send string for the optional XML Broker monitor

◆ Important

The variables in Red text should be replaced as applicable for your deployment.

The following is the Receive String for this monitor:

```
<MPSError type="IMA">0x80130007</MPSError>
```

Figure 2.12 Send string for the optional XML Broker monitor

When configuring this monitor on the BIG-IP LTM, the **User Name** should be **user**, and the **Password** should be **password**.
In the **Reverse** row, click the **Yes** button.

XML Broker Credential Validation health monitor 2

This health monitor tests that the XML Broker is capable of validating real user credentials. This monitor sends a **RequestValidateCredentials** request with a real user name, password, and domain name. These credentials will be passed in clear text, so if that is a security concern for your organization, the previous monitor may be preferable. In this case, we configure the monitor as a reverse monitor and mark the server down when the receive string, **<ErrorId>**, is returned. This string will only exist in the response if a failure occurs. For this health monitor, make certain to replace the user name, password, and domain name with valid entries and edit the Content-Length value to match.

The following is the code for the Send String in this monitor:

```
POST /scripts/wpnbr.dll HTTP/1.1\r\nContent-Type:
text/xml\r\nHost: 10.133.40.100\r\nContent-Length:
329\r\n\r\n<?xml version="1.0"
encoding="UTF-8"?\>\n<!DOCTYPE NFuseProtocol SYSTEM
"NFuse.dtd"\>\n<NFuseProtocol version="4.6"\>\n
<RequestValidateCredentials>\n <Credentials>\n
<UserName>user</UserName>\n <Password
encoding="cleartext">Password</Password>\n
<Domain>citrix</Domain>\n </Credentials>\n
</RequestValidateCredentials>\n</NFuseProtocol>\n
```

Figure 2.13 Send string for the optional XML Broker monitor

◆ Important

The variables in Red text should be replaced as applicable for your deployment.

The following is the Receive String for this monitor:

```
<ErrorId>
```

Figure 2.14 Send string for the optional XML Broker monitor

When configuring this monitor on the BIG-IP LTM, from the **Reverse** row, click the **Yes** button.

Appendix C: Overview of Citrix Presentation Server environment

Citrix Presentation Server allows users to access and run applications hosted on a server or a farm of servers running Citrix Presentation Server software. In a Citrix Presentation Server environment, almost all of the application processing occurs on the server with only keystrokes, mouse-clicks and screen updates being exchanged by the client and the server. A Citrix Presentation Server farm is a grouping of multiple servers running the Citrix Presentation Server software, administered as a single entity.

A typical Citrix Presentation Server environment that allows users to access the applications using a web browser consists of the following components:

- Citrix Web Interface
- Citrix Presentation Server XML Brokers
- Citrix Presentation Server Zone Data Collectors
- Citrix Presentation Server farm

The Citrix Web Interface allows users to access applications hosted on the Citrix Presentation Server farm using a web browser. The Citrix Web Interface runs on a separate Web Server, such as a Microsoft Windows 2003 server running IIS. The Citrix Web Interface retrieves a list of applications hosted on the Citrix Presentation Server farm that the user can access, and publishes them as HTML pages that the users can view in a standard web browser.

The Citrix Web Interface servers and the Citrix Presentation Server farm communicate using the Citrix XML Service. The Citrix XML Service is a component of the Citrix Presentation Server and is present on all the Citrix Presentation Servers as well as the Citrix Web Interface servers. The Citrix XML Service wraps responses from IMA operations such as retrieving a list of applications that a user has access to, server address resolution among others, and encodes them into XML to be transmitted over HTTP.

In large deployments, a small number of Citrix Presentation Servers are designated as XML Brokers, dedicated to collecting data from other servers in the farm, such as the list of applications hosted on the farm that are available to the client. In such large deployments, the Citrix XML Brokers typically also act as the Zone Data Collectors to determine the least busy servers in the farm that can serve the applications, and providing the requested information to the Web Interface servers. One of the primary functions of the Citrix Zone Data Collector is to identify the least busy server within the farm or zone for a published application, send an IMA ping to ensure that the server is alive, and in case the target server has multiple IP Addresses determine the appropriate IP Address for the given client IP, before returning the target address to the XML Broker.

The following diagram illustrates the logical data flow between the client, the Citrix Web Interface and the Citrix Presentation Server farm.

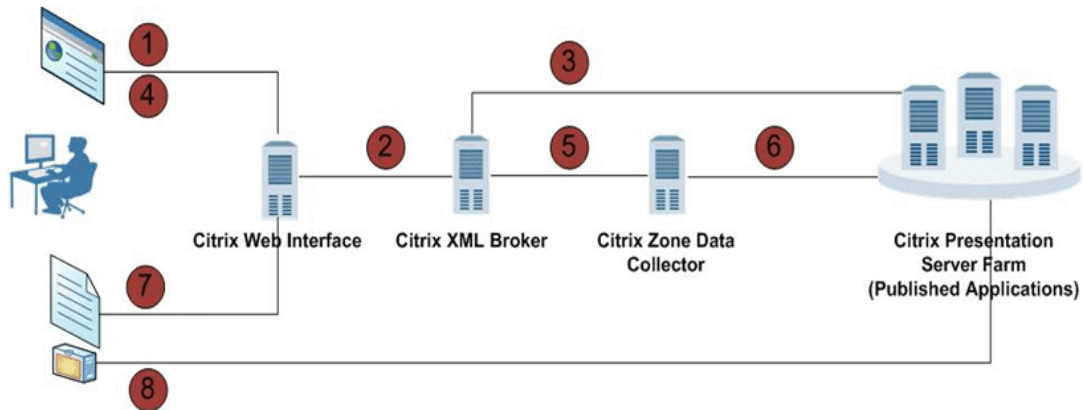


Figure 2.15 Data flow in a Citrix Presentation Server environment

1. The user initiates request for applications by sending credentials to the Web Interface, using a web browser.
2. The Web Interface sends an application retrieval request with the user's credentials to the XML Broker using the XML Service.
3. The XML Broker authenticates the user and retrieves the list of applications that the user can access from the Presentation Server Farm. The XML Broker returns the information about each application the user has access to, to the Web Interface using the XML Service. The Web Interface then publishes a HTML page with the application list to the user.
4. When the user clicks on an application icon on the HTML page, the Web Interface receives this request and uses the XML service to query the XML Broker for the address of the target Presentation Server that the user should connect to.
5. The XML Broker uses the IMA Service to request the target server information from the Zone Data Collector.
6. The Zone Data Collector identifies the address of the least busy Presentation Server hosting the application, sends an IMA ping to ensure that the server is alive, and returns it back to the XML Broker. The XML Broker relays the location of the least busy Presentation Server to the Web Interface using the XML Service.
7. The Web Interface generates a customized ICA file necessary to launch the application and delivers it to the user via the web browser.
8. The ICA file is executed by the client and the user initiates an ICA connection with the target Presentation Server hosting the application.

For more information on Citrix Presentation Server, see
www.citrix.com/English/ps2/products/product.asp?contentID=186

◆ **Note**

On February 11, 2008, Citrix changed the name of its Presentation Server product line to XenApp. This document is written with the assumption that you are familiar with the Citrix Presentation Server software. For more information on configuring the product, consult the appropriate documentation