



Deploying the BIG-IP LTM v9.x with
Microsoft Windows Server 2008
Terminal Services



Microsoft[®] Partner

Deploying the BIG-IP LTM system and Microsoft Windows Server 2008 Terminal Services

Welcome to the BIG-IP LTM- Microsoft® Windows® Server 2008 - Terminal Services Deployment Guide. This guide gives you step-by-step configuration procedures for configuring the BIG-IP LTM (Local Traffic Manager) for directing traffic and maintaining persistence to Microsoft Windows Terminal Services devices.

Terminal Services in Windows Server 2008 enables users to remotely access full Windows desktops, or individual Windows-based applications, on Terminal Server computers. In an environment using BIG-IP LTM system, a farm of terminal servers have incoming connections distributed in a balanced manner across the servers in the farm. Additionally, BIG-IP LTM can offload SSL processing and distribute load for the new Gateway and Web Access roles in Terminal Services.

For more information on Microsoft Windows Server 2008, including Windows Terminal Services, see

<http://www.microsoft.com/windowsserver2008/default.msp>

For more information on the BIG-IP LTM system, see

<http://www.f5.com/products/bigip/lm/>.

This Deployment Guide is broken up into three sections:

- *Configuring the BIG-IP LTM with Windows Server 2008 Terminal Services, including RemoteApp*, on page 5
- *Configuring the BIG-IP LTM system for deployment with the Gateway server role*, on page 14
- *Configuring the BIG-IP LTM system with the Web Access server role*, on page 24

Prerequisites and configuration notes

The following are prerequisites for this deployment:

- ◆ The BIG-IP LTM system should be running version 9.4.2 or later.
- ◆ This Deployment Guide is written for Windows Server 2008 Terminal Services. If you are using Windows Server 2003 Terminal Services, see **<http://www.f5.com/pdf/deployment-guides/wts-bigip9-dg.pdf>**
- ◆ Briefly review the basic configuration tasks and the few pieces of information, such as IP addresses, that you should gather in preparation for completing this configuration.
- ◆ You should be familiar with both the BIG-IP LTM system and Windows Server 2008 Terminal Services. For more information on configuring these products, consult the appropriate documentation.
- ◆ If you are using IPv6 addresses, you must have the IPv6 Gateway module licensed on the BIG-IP LTM system.

Special note about Session Broker Servers

The Session Broker role, new to Windows Server 2008 Terminal Servers, provides simple load balancing and user persistence to farms of Terminal Server computers. BIG-IP LTM, used in conjunction with a Session Broker server, fully supports Session Broker persistence tokens. The BIG-IP LTM also provides additional options and scalability beyond that which Session Broker offers alone:

- Microsoft documentation states that the Session Broker "provides significant value to farms of two to five servers." The BIG-IP LTM can scale efficiently to much higher numbers of servers.
- The BIG-IP LTM offers additional load balancing methods beyond just least connections or predetermined ratios; for instance, an administrator can choose to send new connections to those servers that are observed to be exhibiting the fastest response.

Complete instructions for installing and configuring Session Broker servers can be found in this [*Microsoft TechNet*](#) article. There are a few configuration notes you must make sure to follow.

- ◆ Each Terminal Server computer in this deployment should be enrolled in a session broker farm.
- ◆ You must disable Session Broker load balancing on each of the Session Broker farm members.
- ◆ Clear the **Use IP Address Redirection** box on each Session Broker farm member.
- ◆ You must select a single IP address on each farm member that will be used for reconnection. The IP address you select must be the same address that you configure as a pool member on the BIG-IP LTM, as described in *Creating the pool*, on page 7.

In Figure 1, you see a screen shot of the TS Session Broker properties. In this example, the farm member has been properly configured to work with BIG-IP LTM. The server has IPv4 address of 10.133.22.117, which is also configured as a pool member address on the BIG-IP LTM system. Also notice that **Participate in Session Broker Load-Balancing** and **Use IP Address Redirection** are not checked, as described in the preceding configuration notes.

Refer to the Microsoft documentation for information on how to configure the TS Session Broker properties.

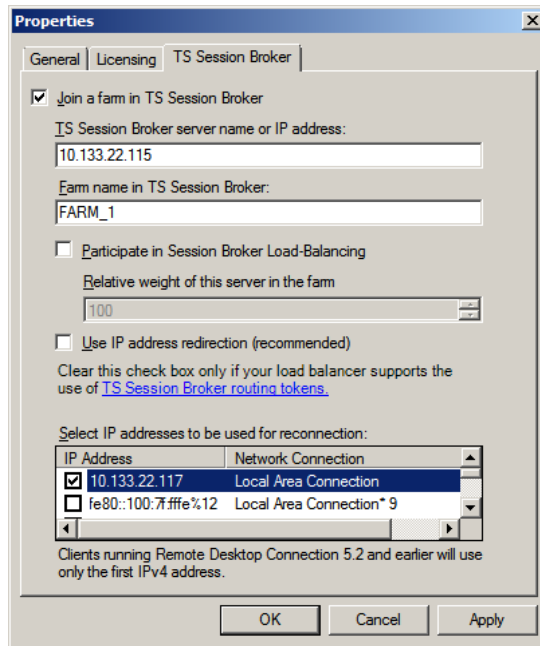


Figure 1 Configuring the TS Session Broker properties

Configuration example

In the scenario used in this Deployment Guide, users connect to a virtual server (single IP address) on the BIG-IP LTM system using the Microsoft Remote Desktop Connection client. The connections are load balanced to a farm of devices running Microsoft Windows Terminal Server. The farm is managed by a Session Broker server, which works in conjunction with the BIG-IP LTM system to ensure that each client connects to the same member of the farm (using persistence on the BIG-IP LTM), across multiple sessions, in order to keep consistent application and data presented to each user.

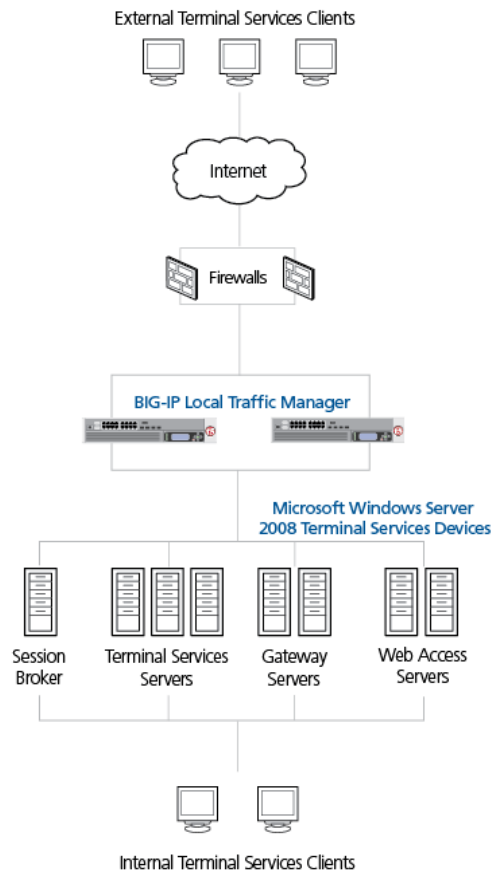


Figure 2 Logical configuration example

◆ Note

The example in Figure 1 is a logical representation of this deployment. Your configuration may be dramatically different than the one shown.

Configuring the BIG-IP LTM with Windows Server 2008 Terminal Services, including RemoteApp

In this section, we configure the BIG-IP LTM system for full Terminal Server sessions, which also supports RemoteApp programs that are accessed through the Terminal Services Remote Desktop Protocol. Unlike full Terminal Server sessions, RemoteApp programs run side-by-side with local programs, and do not require a full remote desktop environment. BIG-IP LTM can direct traffic to servers providing traditional Terminal Services sessions, and those that provide RemoteApp programs, in exactly in the same manner.

More information on deploying RemoteApp programs can be found in this [Microsoft TechNet](#) article.

To configure the BIG-IP LTM system for integration with Windows Terminal Services, you must complete the following procedures:

- *Connecting to the BIG-IP LTM device*
- *Creating the HTTP health monitor*
- *Creating the pool*
- *Creating profiles*
- *Creating the virtual server*

These procedures assume that the Terminal Services clients are coming in from outside the corporate network. If users are also connecting from inside the corporate network, be sure to see *Deploying the BIG-IP LTM for internal users of Windows Terminal services*, on page 13.

◆ Tip

*We recommend you save your existing BIG-IP configuration before you begin the procedures in this Deployment Guide. To save your BIG-IP configuration, see **Appendix A: Backing up and restoring the BIG-IP LTM system configuration**, on page 1-32.*

The BIG-IP LTM system offers both web-based and command line configuration tools, so that users can work in the environment that they are most comfortable with. This Deployment Guide contains procedures to configure the BIG-IP LTM system using the BIG-IP web-based Configuration utility only. If you are familiar with using the **bigpipe** command line interface you can use the command line to configure the BIG-IP device; however, we recommend using the Configuration utility.

Connecting to the BIG-IP LTM device

Use the following procedure to access the BIG-IP web-based Configuration utility using a web browser.

To connect to the BIG-IP LTM system using the Configuration utility

1. In a browser, type the following URL:
https://<administrative IP address of the BIG-IP device>
A Security Alert dialog box appears, click **Yes**.
The authorization dialog box appears.
2. Type your user name and password, and click **OK**.
The Welcome screen opens.

Once you are logged onto the BIG-IP LTM system, the Welcome screen of the new Configuration utility opens. From the Configuration utility, you can configure and monitor the BIG-IP LTM system, as well as access online help, download SNMP MIBs and Plug-ins, and even search for specific objects.

Creating the TCP health monitor

The first step in this configuration is to set up a health monitor for the Windows Terminal Services devices. This procedure is optional, but very strongly recommended.

To create a health monitor

1. On the Main tab, expand **Local Traffic**, and then click **Monitors**.
The Monitors screen opens.
2. Click the **Create** button. The New Monitor screen opens.
3. In the **Name** box, type a name for the Monitor.
In our example, we type **wts-tcp**.
4. From the **Type** list, select **tcp**.
The TCP Monitor configuration options appear.
5. In the Configuration section, in the **Interval** and **Timeout** boxes, type an Interval and Timeout. We recommend at least a 1:3 +1 ratio between the interval and the timeout (for example, the default setting has an interval of **5** and an timeout of **16**). In our example, we use a **Interval** of **30** and a **Timeout** of **91**.
6. In the **Send String** and **Receive Rule** sections, you can add an optional send string and receive rule specific to the device being checked.
7. Click the **Finished** button (see Figure 3).
The new monitor is added to the Monitor list.

Figure 3 Creating the TCP Monitor

Creating the pool

The next step in this configuration is to create a pool on the BIG-IP LTM system for the Windows Terminal Servers. A BIG-IP pool is a set of devices grouped together to receive traffic according to a load balancing method. In this configuration, we create one pool for the Windows Terminal Servers.

To create the Terminal Services 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.

*Note: For more (optional) pool configuration settings, from the Configuration list, select **Advanced**. Configure these settings as applicable for your network.*

3. In the **Name** box, enter a name for your pool. In our example, we use **wts-rdp-pool**.
4. In the **Health Monitors** section, select the name of the monitor you created in the *Creating the HTTP health monitor* section, and click the Add (<<) button. In our example, we select **wts-tcp**.
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 (node)**.

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, add the first server to the pool. In our example, we type **10.133.22.117**
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 **3389**, the default port for RDP.
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 twice for the remaining servers, **10.133.22.118** and **10.133.22.119**.
12. Click the **Finished** button (see Figure4).

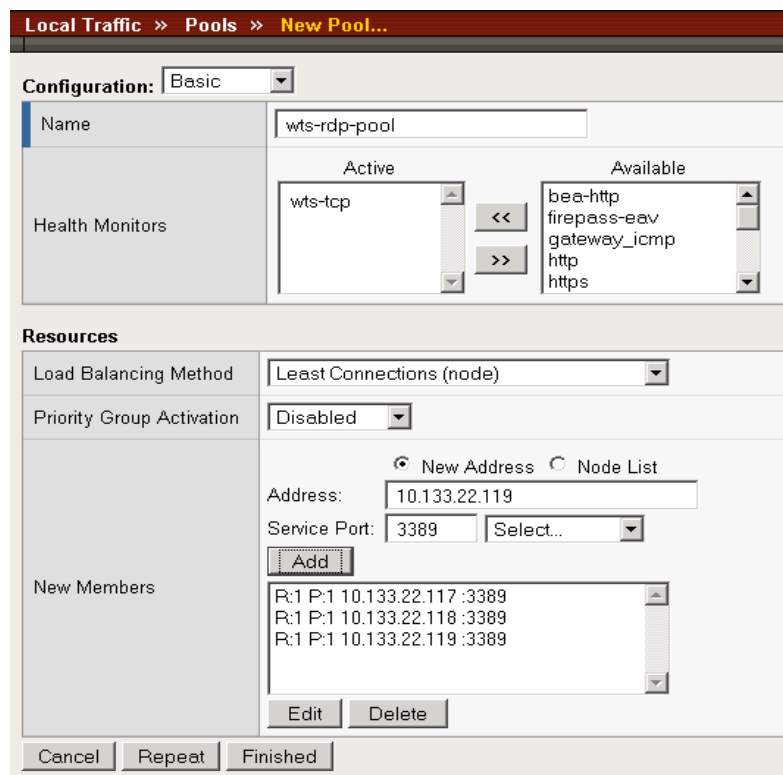


Figure 4 Creating the pool in the BIG-IP Configuration utility

Creating profiles

BIG-IP version 9.0 and later uses profiles. 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. Using profiles enhances your control over managing network traffic, and makes traffic-management tasks easier and more efficient.

Although it is possible to use the default profiles, we strongly recommend you create new profiles based on the default parent profiles. Creating new profiles allows you to easily modify the profile settings specific to this deployment, and ensures you do not accidentally overwrite the default profile.

These profiles use new optimized profiles available in BIG-IP LTM version 9.4 and later. If you are using a BIG-IP LTM version prior to 9.4, the *Configuration Guide for BIG-IP Local Traffic Management* for version 9.4 (available on AskF5) shows the differences between the base profiles and the optimized profile types. Use this guide to manually configure the optimization settings.

Creating a persistence profile

The first profile we create is a persistence profile. The BIG-IP LTM system includes a profile specifically designed for Microsoft Terminal Services: Microsoft Remote Desktop persistence.

In this profile, we suggest choosing a suitably long timeout to accommodate Remote Desktop Protocol client usage patterns. In our example, we've selected 86400 seconds (24 hours); you may find that longer or shorter timeouts are appropriate for your environment.

To create a new 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 **wts-rdp**.
5. From the **Persistence Type** list, select **Microsoft® Remote Desktop** (see Figure 5). The configuration options for Microsoft Remote Desktop persistence appear.
6. In the **Timeout** row, click the Custom box. In the **Seconds** box, type **86400**.
7. Modify any of the settings as applicable for your network.

- Click the **Finished** button.

The screenshot shows a configuration window with two main sections: 'General Properties' and 'Configuration'.

General Properties:

- Name:** wts-rdp
- Persistence Type:** Microsoft® Remote Desktop
- Parent Profile:** msrdp

Configuration: (Custom)

| | | |
|------------------------------|---|-------------------------------------|
| Match Across Services | <input type="checkbox"/> | <input type="checkbox"/> |
| Match Across Virtual Servers | <input type="checkbox"/> | <input type="checkbox"/> |
| Match Across Pools | <input type="checkbox"/> | <input type="checkbox"/> |
| Timeout | Specify... 300 seconds | <input checked="" type="checkbox"/> |
| Has Session Directory | <input checked="" type="checkbox"/> Enabled | <input type="checkbox"/> |

Buttons at the bottom: Cancel, Repeat, Finished

Figure 5 Configuring Microsoft Remote Desktop persistence

Creating the TCP profiles

The next profiles we create are the TCP profiles. For this configuration, we recommend two different TCP profiles, one for the client and one for the server. We recommend a WAN optimized TCP profile for the client, and a LAN optimized profile for the server.

Creating the WAN optimized TCP profile

First we configure the WAN optimized profile.

To create a new TCP WAN optimized profile

- On the Main tab, expand **Local Traffic**, and then click **Profiles**. The HTTP Profiles screen opens.
- On the Menu bar, from the **Protocol** menu, click **tcp**.
- In the upper right portion of the screen, click the **Create** button. The New TCP Profile screen opens.
- In the **Name** box, type a name for this profile. In our example, we type **wts-rdp-wan**.
- From the **Parent Profile** list, select **tcp-wan-optimized**.
- In the **Idle Timeout** row, click the Custom box. In the **Seconds** box, type **86400**.
- Modify any of the settings as applicable for your network. In our example, we leave the settings at their default levels.
- Click the **Finished** button.

Creating the LAN optimized TCP profile

First we configure the LAN optimized profile. If you are not using version 9.4 or 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. 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 **wts-rdp-lan**.
5. From the **Parent Profile** list, select **tcp-lan-optimized** if you are using BIG-IP LTM version 9.4 or later; otherwise select **tcp**.
6. In the **Idle Timeout** row, click the Custom box. In the **Seconds** box, type **86400**.
7. Modify any of the settings as applicable for your network. In our example, we leave the settings at their default levels.
8. Click the **Finished** button.

Creating the virtual server

Next, we configure a virtual server that references the profiles and pool you created in the preceding procedures.

To create the 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 **wts-rdp-vs**.
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**.

- In the **Service Port** box, type **3389**.

| General Properties | |
|--------------------|---|
| Name | wts-rdp-vs |
| Destination | Type: <input checked="" type="radio"/> Host <input type="radio"/> Network |
| | Address: 172.27.92.118 |
| Service Port | 3389 Other: <input type="text"/> |
| State | Enabled |

Figure 6 Adding the Terminal Services virtual server

- From the **Protocol Profile (Client)** list, select the profile you created in the *Creating the WAN optimized TCP profile* section. In our example, we select **wts-rdp-wan**.
- From the **Protocol Profile (Server)** list, select the profile you created in the *Creating the LAN optimized TCP profile* section. In our example, we select **wts-rdp-lan**.
- In the Resources section, from the **Default Pool** list, select the pool you created in the *Creating the pool* section. In our example, we select **wts-rdp-pool**.
- From the **Default Persistence Profile** list, select the persistence profile you created in the *Creating a persistence profile* section. In our example, we select **wts-rdp**.
- Click the **Finished** button.

| Resources | |
|---|--------------|
| iRules | Enabled |
| | Available |
| HTTP Class Profiles | Enabled |
| | Available |
| Default Pool | wts-rdp-pool |
| Default Persistence Profile | wts-rdp |
| Fallback Persistence Profile | None |
| <input type="button" value="Cancel"/> <input type="button" value="Repeat"/> <input type="button" value="Finished"/> | |

Figure 7 Resources section of the add virtual server page

Deploying the BIG-IP LTM for internal users of Windows Terminal services

If your deployment includes internal users of Windows Server 2008 Terminal Services, you must create another virtual server and the associated objects for these users which will be optimized for LAN traffic.

Creating the health monitor

To create the health monitor, follow *Creating the HTTP health monitor*, on page 16. You can alternatively use the same health monitor you created previously, however we recommend creating a new health monitor.

Creating the pool

To create the pool, follow *Creating the pool*, on page 7. When configuring the pool, add the health monitor you created in the preceding procedure.

Creating the profiles

For internal users, we create two profiles, a persistence profile and a LAN optimized TCP profile. Again, you can use the same profiles you created previously, however we recommend creating new profiles.

To create the persistence profile, follow *Creating a persistence profile*, on page 9.

To create the LAN optimized TCP profile, follow *Creating the LAN optimized TCP profile*, on page 11.

Creating the virtual server

To create the virtual server, follow *Creating the virtual server*, on page 11. Use the appropriate IP address. From the **Protocol Profile (Client)** list, select the LAN optimized profile you created in the preceding procedure. Leave the **Protocol Profile (Server)** list at the default setting (Use Client Profile). Add the pool and persistence profile you created for the internal users.

This completes the configuration for the internal users of Windows 2008 Terminal Services.

Configuring the BIG-IP LTM system for deployment with the Gateway server role

The Gateway role, new to Windows Server 2008 Terminal Services, allows authorized users to tunnel Remote Desktop Protocol (RDP) connections over HTTPS, using the standard Terminal Services client. Benefits of Gateway servers include: remote access without the use of a VPN solution; the ability to connect from remote networks that do not allow RDP connections (TCP port 3389) through their firewalls; comprehensive control over user access policies; and publication of a single name and address to the public networks, rather than one for each internal Terminal Server resource. More information on deploying Gateway Servers can be found in this [Microsoft TechNet](#) article.

Prerequisites and configuration notes

The following are prerequisites for this section:

- ◆ Administrators must enable **HTTPS-HTTP Bridging** on Gateway servers to enable offloading of SSL/TLS.
- ◆ Administrators must add each Gateway Server to a TS Gateway Server farm. The list of farm members must be identical on each Gateway server.

In the following screenshots, we show an example of a Gateway server that has been properly configured to participate in a TS Gateway server farm. In Figure 8, you can see that **HTTPS-HTTP Bridging** has been enabled. Figure 9 shows that two members have been added to the farm. In this example, we show the IPv6 addresses for the farm members, but the procedure is the same for IPv4 addressing.

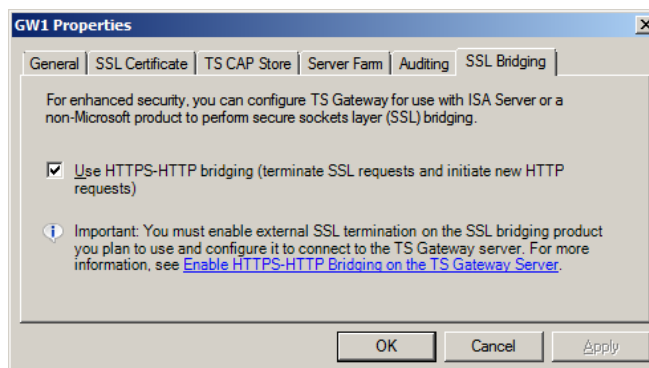


Figure 8 Configuring HTTPS-HTTP bridging on the TS Gateway server

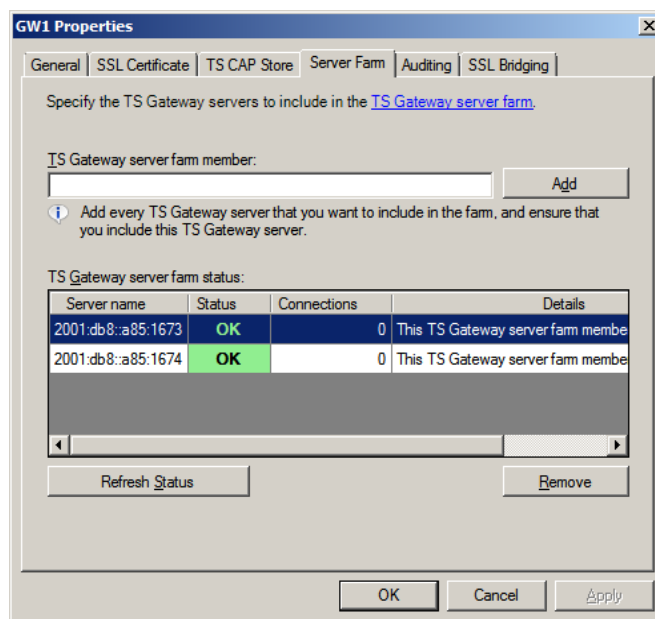


Figure 9 Configuring the Server Farm properties

For more information on configuring the Gateway Server role, see the Microsoft documentation.

Connecting to the BIG-IP LTM device

Use the following procedure to access the BIG-IP web-based Configuration utility using a web browser.

To connect to the BIG-IP LTM system using the Configuration utility

1. In a browser, type the following URL:
https://<administrative IP address of the BIG-IP device>
 A Security Alert dialog box appears, click **Yes**.
 The authorization dialog box appears.
2. Type your user name and password, and click **OK**.
 The Welcome screen opens.

Once you are logged onto the BIG-IP LTM system, the Welcome screen of the new Configuration utility opens. From the Configuration utility, you can configure and monitor the BIG-IP LTM system, as well as access online help, download SNMP MIBs and Plug-ins, and even search for specific objects.

Importing keys and certificates

Before you can enable the BIG-IP LTM system to offload SSL traffic from Gateway servers, you must install a SSL certificate and key on the BIG-IP LTM system. 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 system to generate a request for a new certificate and key from a certificate authority, see the Managing SSL Traffic chapter in the *Configuration Guide for Local Traffic Management*.

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

To import a key or certificate

1. On the Main tab, expand Local Traffic.
2. Click **SSL Certificates**.
This displays the list of existing certificates.
3. In the upper right corner of the screen, click **Import**.
4. From the **Import Type** list, select the type of import (**Certificate** or **Key**).
5. In the **Certificate** (or **Key**) **Name** box, type a unique name for the certificate or key.
6. In the **Certificate** (or **Key**) **Source** box, choose to either upload the file or paste the text.
7. Click **Import**.

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

Creating the HTTP health monitor

The next step in this configuration is to set up a health monitor for the Gateway servers. This procedure is optional, but very strongly recommended.

To create a health monitor

1. On the Main tab, expand **Local Traffic**, and then click **Monitors**.
The Monitors screen opens.
2. Click the **Create** button. The New Monitor screen opens.
3. In the **Name** box, type a name for the Monitor.
In our example, we type **wts-gateway-http**.
4. From the **Type** list, select **http**.
The TCP Monitor configuration options appear.

-
5. In the Configuration section, in the **Interval** and **Timeout** boxes, type an Interval and Timeout. We recommend at least a 1:3 +1 ratio between the interval and the timeout (for example, the default setting has an interval of **5** and an timeout of **16**). In our example, we use a **Interval** of **30** and a **Timeout** of **91**.
 6. In the **Send String** and **Receive Rule** sections, you can add an optional send string and receive rule specific to the device being checked.
 7. Click the **Finished** button.
The new monitor is added to the Monitor list.

Creating the pool

The next step in this configuration is to create a pool on the BIG-IP LTM system for the Windows Terminal Servers.

In the following example, we use IPv6 addresses for the nodes. This is not a requirement, and is done to show how to configure a pool using IPv6 addresses. Enter the IP address type appropriate for your configuration.

◆ Note

When using different address types for virtual servers and nodes (for example, when the BIG-IP LTM provides an IPv4 virtual server for IPv6 nodes), the LTM performs source-NATing of the client IP address regardless of whether or not a SNAT policy has been set. By default, the SNAT is set to the local self-IP of the LTM on the network that communicates with the destination nodes, and is of the same format as the destination.

For instance, an IPv6 node results in incoming client connections being SNATed to the IPv6 self-IP of the LTM on the network which carries that IPv6 traffic. To override the SNAT behavior with your own selection of addresses, which still must be of the appropriate address type, configure a SNAT profile and apply it to the virtual server.

To create the Gateway 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.

***Note:** For more (optional) pool configuration settings, from the Configuration list, select **Advanced**. Configure these settings as applicable for your network.*

3. In the **Name** box, enter a name for your pool.
In our example, we use **wts-gateway-IPv6**.

4. In the **Health Monitors** section, select the name of the monitor you created in the *Creating the HTTP health monitor* section, and click the Add (<<) button. In our example, we select **wts-gateway-http**.
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 (node)**.
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, add the first server to the pool. In our example, we type the following IPv6 address: **2001:db8:0:0:0:0:a85:1673**
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 once for **2001:db8:0:0:0:0:a85:1674**.
12. Click the **Finished** button (see Figure 10).

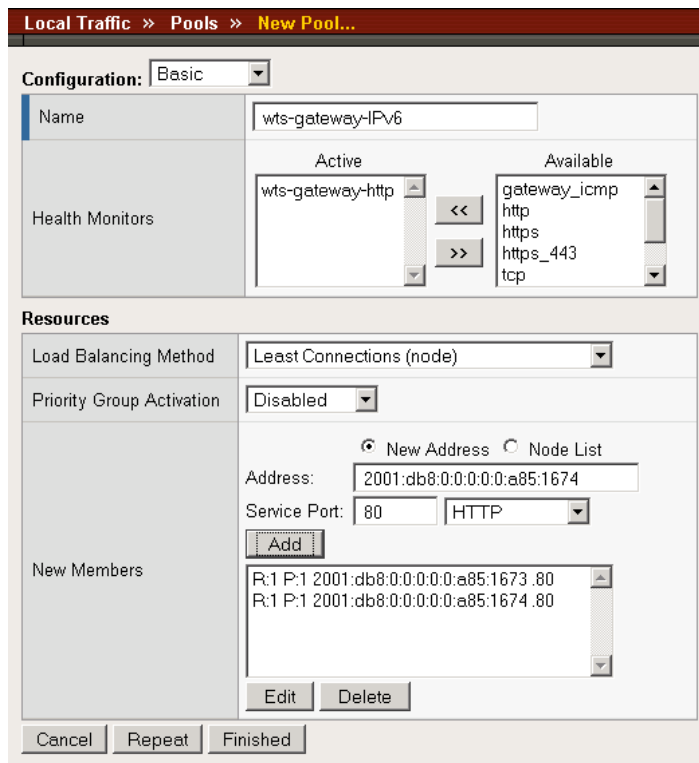


Figure 10 Creating the Gateway IPv6 pool

Creating the iRule

The next object we configure is an iRule that is used for persistence. This iRule is necessary because Microsoft Remote Desktop protocol does not support HTTP cookies, so the BIG-IP LTM persists based on this rule. In some cases you may be able to use other persistence methods such as Source Address Affinity, which bases persistence on the IP address of the client. However, because proxy servers or NAT (network address translation) devices may aggregate clients behind a single IP address, such methods are not always effective. To ensure reliable persistence, we recommend using the following iRule and associated persistence profile.

To create the iRule

1. On the Main tab, expand **Local Traffic**, and then click **iRules**. The Virtual Servers screen opens.
2. In the upper right portion of the screen, click the **Create** button. The New iRule screen opens.
3. In the **Name** box, type a name for this iRule. In our example, we type **PersistRule**.
4. In the Definition box, copy and paste the following iRule:

```
when HTTP_REQUEST {  
    if { [HTTP::header exists "Authorization"] } {  
        persist uie [HTTP::header "Authorization"]  
    }  
}
```

5. Click the **Finished** button.

Creating profiles

For the Gateway servers, we create five profiles: persistence, HTTP, two TCP profiles, and a Client SSL profile. As previously mentioned, you can use the default profiles if you are not changing any of the settings; however we strongly recommend creating new profiles.

Creating the persistence profile

The first profile we create is a persistence profile. This profile uses the iRule you created in *Creating the iRule*, on page 19.

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 **wts-gateway-persist**.
5. From the **Persistence Type** list, select **Universal**. The configuration options for universal persistence appear.
6. Click the Custom boxes for **iRule** and **Timeout**.
7. From the iRule list, select the name of the iRule you created in *Creating the iRule*, on page 19. In our example, we select **PersistRule**.
8. In the **Timeout** box, type **3600** seconds (one hour).
9. Click the **Finished** button.

| General Properties | |
|--------------------|---------------------|
| Name | wts-gateway-persist |
| Persistence Type | Universal |
| Parent Profile | universal |

| Configuration | | Custom <input checked="" type="checkbox"/> |
|------------------------------|--------------------------|--|
| Match Across Services | <input type="checkbox"/> | <input type="checkbox"/> |
| Match Across Virtual Servers | <input type="checkbox"/> | <input type="checkbox"/> |
| Match Across Pools | <input type="checkbox"/> | <input type="checkbox"/> |
| iRule | PersistRule | <input checked="" type="checkbox"/> |
| Timeout | Specify... 3600 seconds | <input checked="" type="checkbox"/> |

Cancel Repeat Finished

Figure 11 Configuring the persistence profile

Creating an HTTP profile

The next profile we create is an HTTP profile. In the following example, we base our HTTP profile off of a new profile included with BIG-IP LTM version 9.4, called **http-wan-optimized-compression-caching**. This profile includes some default optimization settings that increase performance over the WAN.

There are a couple of caveats for using this profile:

- ◆ You must have Compression and RAM Cache licensed on your BIG-IP LTM system. Contact your Sales Representative for more information.
- ◆ This profile is only available in BIG-IP LTM version 9.4 and later.

To create a new HTTP profile

1. On the Main tab, expand **Local Traffic**.
2. Click **Profiles**.
The HTTP Profiles screen opens.
3. In the upper right portion of the screen, click the **Create** button.
The new HTTP Profile screen opens.
4. In the **Name** box, type a name for this profile. In our example, we type **wts-gateway-http**.
5. From the Parent Profile list, select **http-wan-optimized-compression-caching**.
6. Modify any of the other options as applicable for your configuration. See the online help for more information on the configuration options.
7. Click the **Finished** button.

Creating the TCP profiles

The next profiles we create are the TCP profiles. For this configuration, we recommend two different TCP profiles, one for the client and one for the server. We recommend a WAN optimized TCP profile for the client, and a LAN optimized profile for the server.

In our example, we leave these profiles at their default levels; you can configure any of the options as applicable for your network.

Creating the WAN optimized TCP profile

First we configure the WAN optimized 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 **wts-gateway-wan**.
5. From the **Parent Profile** list, select **tcp-wan-optimized**.
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 LAN optimized TCP profile

First we configure the LAN optimized profile. If you are not using version 9.4 or 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. 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 **wts-gateway-lan**.
5. From the **Parent Profile** list, select **tcp-lan-optimized** if you are using BIG-IP LTM version 9.4 or later; otherwise select **tcp**.
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 a Client SSL profile

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

To create a new Client SSL profile

1. On the Main tab, expand **Local Traffic**.
2. Click **Profiles**. The HTTP Profiles screen opens.
3. On the Menu bar, from the **SSL** menu, select **Client**. The Client SSL Profiles screen opens.
4. In the upper right portion of the screen, click the **Create** button. The New Client SSL Profile screen opens.
5. In the **Name** box, type a name for this profile. In our example, we type **wts-gateway-ssl**.
6. In the Configuration section, click a check in the **Certificate** and **Key** Custom boxes.
7. From the **Certificate** list, select the name of the Certificate you imported in the *Importing keys and certificates* section.
8. From the **Key** list, select the key you imported in the *Importing keys and certificates* section.
9. Click the **Finished** button.

Creating the virtual server

Next, we configure a virtual server that references the profiles and pool you created in the preceding procedures.

To create the 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 **wts-gateway-vs**.
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 **10.133.22.132**.
6. In the **Service Port** box, type **443**.
7. From the **Protocol Profile (Client)** list, select the profile you created in *Creating the WAN optimized TCP profile*, on page 21. In our example, we select **wts-gateway-wan**.
8. From the **Protocol Profile (Server)** list, select the profile you created in *Creating the LAN optimized TCP profile*, on page 22. In our example, we select **wts-gateway-lan**.
9. From the **HTTP Profile** list, select the profile you created in *Creating an HTTP profile*, on page 20. In our example, we select **wts-gateway-http**.
10. From the **SSL Profile (Client)** list, select the profile you created in *Creating a Client SSL profile*, on page 22. In our example, we select **wts-gateway-ssl**.
11. In the Resources section, from the **Default Pool** list, select the pool you created in *Creating the pool*, on page 17. In our example, we select **wts-gateway-IPv6**.
12. From the **Default Persistence Profile** list, select the persistence profile you created in *Creating the persistence profile*, on page 19. In our example, we select **wts-gateway-persist**.
13. Click the **Finished** button.

This concludes the Windows Server 2008 Terminal Services Gateway Server configuration.

Configuring the BIG-IP LTM system with the Web Access server role

In this section, we configure the BIG-IP LTM for the Web Access server component of Windows Server 2008 Terminal Services. The Web Access role, new to Windows Server 2008 Terminal Servers, allows authorized users to connect to a web site that presents pre-configured icons for access to Terminal Servers, Terminal Server farms, or individual applications that have been made available via RemoteApp functionality. The applications may be made available either directly via RDP, or through a Gateway server.

Note that the Web Access Servers should use a separate LTM virtual server that used for the Gateway servers, whether or not the Gateway roles are installed on the same devices.

Importing keys and certificates

The first step in this configuration is to import the key and certificate.

To import a key or certificate

1. On the Main tab, expand Local Traffic.
2. Click **SSL Certificates**.
This displays the list of existing certificates.
3. In the upper right corner of the screen, click **Import**.
4. From the **Import Type** list, select the type of import (**Certificate** or **Key**).
5. In the **Certificate** (or **Key**) **Name** box, type a unique name for the certificate or key.
6. In the **Certificate** (or **Key**) **Source** box, choose to either upload the file or paste the text.
7. Click **Import**.

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

Creating the HTTP health monitor

The next step is to set up health monitors for the Web Access devices. This procedure is optional, but very strongly recommended. In our example, we create a simple HTTP health monitor. Although the monitor in the following example is quite simple, you can configure optional settings such as Send and Receive Strings to make the monitor much more specific.

To create a health monitor

1. On the Main tab, expand **Local Traffic**, and then click **Monitors**.
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 **wts-wa-http**.
4. From the **Type** list, select **http**.
5. In the Configuration section, in the **Interval** and **Timeout** boxes, type an Interval and Timeout. We recommend at least a 1:3 +1 ratio between the interval and the timeout (for example, the default setting has an interval of **5** and an timeout of **16**). In our example, we use a **Interval** of **30** and a **Timeout** of **91**.
6. In the Send String and Receive Rule sections, you can add a Send String and Receive Rule specific to the device being checked.
7. Click the **Finished** button.
The new monitor is added to the Monitor list.

Creating the pool

The next step is to define a load balancing pool for the Web Access servers.

To create the Web Access 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, type a name for your pool.
In our example, we use **wts-wa-pool**.
4. In the **Health Monitors** section, select the name of the monitor you created in the *Creating the HTTP health monitor* section, and click the Add (<<) button. In our example, we select **wts-wa-http**.
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 (node)**.
6. In 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, add the first Web Access server to the pool. In our example, we type **10.133.22.17**.
9. In the **Service Port** box, type **80** or select **HTTP** from the list.
10. Click the **Add** button to add the member to the list.

11. Repeat steps 8-10 for each server you want to add to the pool.
12. Click the **Finished** button.

Creating profiles

For the Web Access configuration, we create the following profiles: an HTTP profile, two TCP profiles, a persistence profile, a Client SSL profile, and a OneConnect profile.

Creating an HTTP profile

The first new profile we create is an HTTP profile. For deployments where the majority of users accessing the Web Access devices are connecting across a WAN, F5 using a profile introduced in BIG-IP version 9.4 called **http-wan-optimized-compression-caching**. This profile uses specific compression and caching (among other) settings to optimize traffic over the WAN.

If you are not using version 9.4, or do not have compression or caching licensed, you can choose the default HTTP parent profile, or one of the other optimized HTTP parent profiles.

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. The New HTTP Profile screen opens.
3. In the **Name** box, type a name for this profile. In our example, we type **wts-wa-http**.
4. From the **Parent Profile** list, select **http-wan-optimized-compression-caching**.
5. Check the Custom box for **Redirect Rewrite**, and from the **Redirect Rewrite** list, select **Match**.
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 Microsoft IIS 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). In our example, we leave these profiles at their default levels; you can configure any of the options as applicable for your network.

Creating the LAN optimized TCP profile

First we configure the LAN optimized profile. If you are not using version 9.4 or 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. 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 **wts-wa-tcp-lan**.
5. From the **Parent Profile** list, select **tcp-lan-optimized** if you are using BIG-IP LTM version 9.4 or later; otherwise select **tcp**.
6. In the **Idle Timeout** row, click the Custom box. In the **Seconds** box, type **86400**.
7. Modify any of the 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 **wts-wa-tcp-wan**.
5. From the **Parent Profile** list, select **tcp-wan-optimized**.
6. In the **Idle Timeout** row, click the Custom box. In the **Seconds** box, type **86400**.

7. Modify any of the settings as applicable for your network. In our example, we leave the settings at their default levels.
8. Click the **Finished** button.

Creating persistence profile

The next profile we create is a Persistence profile. We recommend using cookie persistence (HTTP cookie insert).

To create a new cookie persistence profile based on the default 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 **wts-wa-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 a Client SSL profile

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

To create a new Client SSL profile

1. On the Main tab, expand **Local Traffic**.
2. Click **Profiles**. The HTTP Profiles screen opens.
3. On the Menu bar, from the **SSL** menu, select **Client**. The Client SSL Profiles screen opens.
4. In the upper right portion of the screen, click the **Create** button. The New Client SSL Profile screen opens.
5. In the **Name** box, type a name for this profile. In our example, we type **wts-wa-ssl**.

-
6. In the Configuration section, click a check in the **Certificate** and **Key Custom** boxes.
 7. From the **Certificate** list, select the name of the Certificate you imported in the *Importing keys and certificates* section.
 8. From the **Key** list, select the key you imported in the *Importing keys and certificates* section.
 9. Click the **Finished** button.

Creating a OneConnect profile

The final profile we create is a OneConnect profile. With OneConnect enabled, client requests can utilize existing, server-side connections, thus reducing the number of server-side connections that a server must negotiate to service those requests. This can provide significant performance improvements for Web Access implementations. For more information on OneConnect, see the BIG-IP LTM documentation.

In our example, we leave all the options at their default settings. You can configure these options as appropriate for your network.

Important

If you configure a OneConnect profile, you must disable Windows Authentication and enable Basic authentication within IIS for the Terminal Server virtual servers on each Web Access node.

To create a new OneConnect profile

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

Creating the virtual server

Next, we configure a virtual server that references the profiles and pool you created in the preceding procedures.

To create the 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 **wts-wa-vs**.
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 **10.133.22.133**.
6. In the **Service Port** box, type **443**, or select **HTTPS** from the list.
Creating the IIS 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 *Creating the WAN optimized TCP profile*, on page 27. If you did not create a WAN optimized profile, select the LAN optimized profile as in the following Step. In our example, we select **wts-wa-tcp-wan**.
10. From the **Protocol Profile (Server)** list, select the name of the profile you created in *Creating the LAN optimized TCP profile*, on page 27. In our example, we select **wts-wa-tcp-lan**.
11. From the **OneConnect Profile** list, select the name of the profile you created in *Creating a OneConnect profile*, on page 29. In our example, we select **wts-wa-oneconnect**.
12. From the HTTP Profile list, select the name of the profile you created in *Creating an HTTP profile*, on page 26. In our example, we select **wts-wa-http**.
13. From the **SSL Profile (Client)** list, select the profile you created in *Creating a Client SSL profile*, on page 28. In our example, we select **wts-wa-ssl**.
14. In the Resources section, from the **Default Pool** list, select the pool you created in *Creating the pool*, on page 25. In our example, we select **wts-wa-pool**.
15. From the **Default Persistence Profile** list, select the persistence profile you created in *Creating persistence profile*, on page 28. In our example, we select **wts-wa-cookie**.
16. Click the **Finished** button.

The BIG-IP LTM configuration for the Microsoft Windows Server 2008 Terminal Services is now complete.

Synchronizing the BIG-IP configuration if using a redundant system

If you are using a redundant BIG-IP configuration, the final step is to synchronize the configuration to the peer BIG-IP device.

To synchronize the configuration using the Configuration utility

1. On the Main tab, expand **System**.
2. Click **High Availability**.
The Redundancy screen opens.
3. On the Menu bar, click **ConfigSync**.
4. Click the **Self --> Peer** button.
The configuration synchronizes with its peer.

Appendix A: Backing up and restoring the BIG-IP LTM system configuration

We recommend saving your BIG-IP configuration before you begin this configuration. When you save the BIG-IP configuration, it collects the following critical data and compress it into a single User Configuration Set (UCS) file:

- BIG-IP configuration files
- BIG-IP license and passwords
- SSL certificates
- SSH keys

Backing up and restoring the BIG-IP LTM configuration

The Configuration Management screen allows you to save and restore all configuration files that you may edit to configure a BIG-IP LTM system. These configuration files are called a User Configuration Set (UCS). The Configuration Management screen contains sections for saving and restoring a configuration. The list boxes in these sections display only files in the `/usr/local/ucs` directory. If you want to save or restore files from another directory, you must type the full path in the box.

To save the BIG-IP configuration using the Configuration utility

1. In the navigation pane, click **System Admin**.
The User Administration screen displays.
2. Click the Configuration Management tab.
The Configuration Management screen displays.
3. In the **Save Current Configuration** section, type the path where you want your configuration file saved or choose a path from the list box. If no path is specified, the BIG-IP saves files to `/usr/local/ucs`. The BIG-IP appends the extension `.ucs` to file names without it. In our example, we type **pre_wts_backup.ucs**.
4. Click the **Save** button to save the configuration file.

To restore a BIG-IP configuration

1. In the navigation pane, click **System Admin**.
The User Administration screen displays.
2. Click the Configuration Management tab.
The Configuration Management screen displays.

-
3. In the **Restore a Configuration** section, choose the configuration file you want to restore from the list box, or type the path where your configuration files were saved.
 4. Click the **Restore** button.
To check the status of the restoration, click the **View Log** button. You should wait a few moments for the log file to start generating before you click **View Log**. Repeated clicking of this button will update your screen with the most current log file information until the restoration is complete.