

## Deployment Guide

# Deploying the BIG-IP System with Microsoft Windows Server 2003 Terminal Services



---

# Deploying the BIG-IP LTM system and Microsoft Windows Server 2003 Terminal Services

Welcome to the BIG-IP - Microsoft® Windows® Server 2003 Terminal Services Deployment Guide. This guide gives you step-by-step configuration procedures for configuring the BIG-IP LTM (Local Traffic Management) system for directing traffic and maintaining persistence to Microsoft Terminal Services devices.

Terminal Services is a technology that lets users run Microsoft Windows-based applications on a remote Windows Server 2003-based computer. In a Terminal Server-based computing environment, all application execution and data processing occur on the server. In an environment using the BIG-IP LTM system, a farm of terminal servers have incoming session connections distributed in a balanced manner across the servers in the farm. The session directory (SD) keeps a list of sessions indexed by user name, and allows a user to reconnect to the terminal server where the user's disconnected session resides and resume that session.

For more information on Microsoft Windows Terminal Services, see <http://www.microsoft.com/windowsserver2003/technologies/terminalservices/default.mspx>

For more information on the BIG-IP LTM system, see <http://www.f5.com/products/big-ip/>.

## Prerequisites and configuration notes

The following are prerequisites for this deployment:

- ◆ The BIG-IP LTM system must be running version 9.1 or later. We recommend version 9.2 or later.
- ◆ A Microsoft Windows Server 2003 with Terminal Server.
- ◆ A Microsoft Windows Server 2003 device configured as a Session Directory Server.
- ◆ All of the configuration procedures in this document are performed on the BIG-IP LTM system. For information on how to deploy or configure Windows Terminal Services, consult the appropriate Microsoft documentation.
- ◆ 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.

### ◆ Note

---

*This document is written with the assumption that you are familiar with both the BIG-IP LTM system and Windows Server 2003 Terminal Services. For more information on configuring these products, consult the appropriate documentation.*

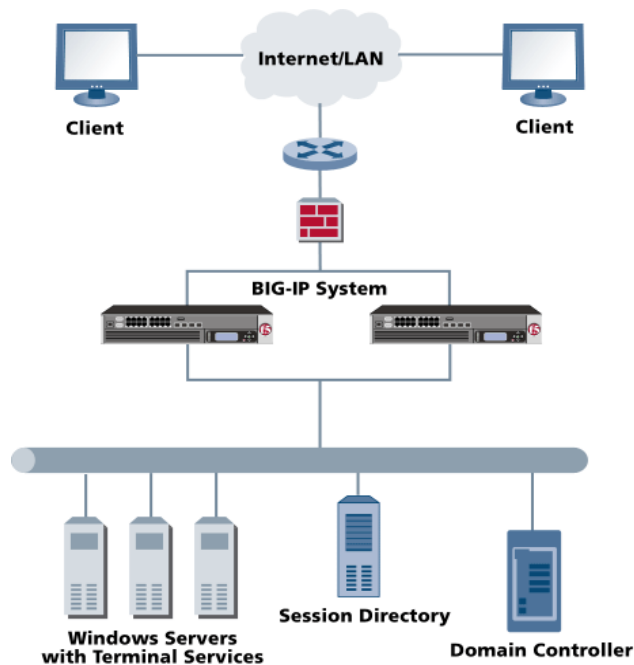
---

## Configuration example

In this scenario, 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 Directory 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.

### ◆ Tip

*Although only one BIG-IP device is necessary for this configuration, we strongly recommend a redundant BIG-IP device for the highest level of availability.*



*Figure 1 BIG-IP Windows Terminal Services 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 system for deployment with Windows Terminal Services

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

- *Connecting to the BIG-IP device*
- *Creating the TCP health monitor*
- *Creating the pool*
- *Creating profiles*
- *Creating the virtual server*
- *Synchronizing the BIG-IP configuration if using a redundant system*

## ◆ 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 10.*

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 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. For this configuration, we use an Extended Content Verification (ECV) monitor, which checks nodes (IP address and port combinations), and can be configured to use **send** and **recv** statements in an attempt to retrieve explicit content from nodes. We configure the health monitors first in version 9.0 and later, as health monitors are now associated at the pool level.

### To configure a health monitor from the BIG-IP 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 **wts\_monitor**.
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.

General Properties	
Name	wts_monitor
Type	TCP
Import Settings	tcp
Configuration: Basic	
Interval	30 seconds
Timeout	91 seconds
Send String	
Receive String	
Reverse	<input type="radio"/> Yes <input checked="" type="radio"/> No
Transparent	<input type="radio"/> Yes <input checked="" type="radio"/> No
<input type="button" value="Cancel"/> <input type="button" value="Repeat"/> <input type="button" value="Finished"/>	

**Figure 2** Creating the TCP Monitor

- 
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. 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 WTS 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\_pool**.
4. In the **Health Monitors** section, select the name of the monitor you created in the *Creating the TCP health monitor* section, and click the Add (<<) button. In our example, we select **wts\_monitor**.
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 **10.133.22.14**.
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**.
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, **10.133.22.15** and **10.133.22.16**.

12. Click the **Finished** button (see Figure3).

The screenshot shows the BIG-IP Configuration utility interface. At the top, the 'Configuration' dropdown is set to 'Basic'. The 'Name' field contains 'wts\_pool'. Under 'Health Monitors', there are two lists: 'Active' containing 'wts\_monitor' and 'Available' containing 'SPSHTTP\_monitor', 'http', 'https', 'https\_443', and 'siebel\_web'. In the 'Resources' section, the 'Load Balancing Method' is 'Least Connections (node)' and 'Priority Group Activation' is 'Disabled'. Under 'New Members', the 'New Address' radio button is selected, with 'Address' set to '10.133.22.16' and 'Service Port' set to '3389'. Below this, a list of members shows three entries: 'R:1 P:1 10.133.22.14:3389', 'R:1 P:1 10.133.22.15:3389', and 'R:1 P:1 10.133.22.16:3389'. At the bottom, there are 'Cancel', 'Repeat', and 'Finished' buttons.

*Figure 3* Creating the wts\_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.

## 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.

---

## 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 4). The configuration options for Microsoft Remote Desktop persistence appear.
6. Modify any of the settings as applicable for your network.
7. Click the **Finished** button.

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"/>

Cancel Repeat Finished

*Figure 4* Configuring Microsoft Remote Desktop persistence

## Creating a TCP profile

For this Deployment Guide, we use the default TCP profile. However, if you want to change any of the default settings, either now or later, we recommend you create a new TCP profile based on the default TCP profile, using the following procedure.

### To create a new TCP profile based on the default TCP profile

1. On the Main tab, expand **Local Traffic**.

2. Click **Profiles**.  
The HTTP Profiles screen opens.
3. On the Menu bar, from the **Protocol** menu, select **TCP**.
4. In the upper right portion of the screen, click the **Create** button.  
The New TCP Profile screen opens.
5. In the **Name** box, type a name for this profile. In our example, we type **wts\_tcp**.
6. Modify any of the settings as applicable for your network.
7. Click the **Finished** button.

For more information on creating or modifying profiles, or applying profiles in general, see the BIG-IP documentation.

## 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\_virtual**.
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 **3389** (see Figure 5).

General Properties	
Name	wts_virtual
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 <input type="text"/>

*Figure 5 Adding the Terminal Services virtual server*

- 
7. If you created a new TCP profile in the preceding procedure, from the Configuration list, select **Advanced**.

From the **Protocol Profile (Client)** list select the name of the profile you created in the Creating a TCP profile section. In our example, we select **wts\_tcp**.

***Important:** This step is only necessary if you created a new TCP profile.*

8. 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\_pool**.
9. 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**.

Resources					
iRules	<table border="1"><thead><tr><th>Enabled</th><th>Available</th></tr></thead><tbody><tr><td></td><td><ul style="list-style-type: none"><li>_sys_auth_ldap</li><li>_sys_auth_radius</li><li>_sys_auth_ssl_cc_ldap</li><li>_sys_auth_ssl_ocsp</li><li>_sys_auth_tacacs</li></ul></td></tr></tbody></table>	Enabled	Available		<ul style="list-style-type: none"><li>_sys_auth_ldap</li><li>_sys_auth_radius</li><li>_sys_auth_ssl_cc_ldap</li><li>_sys_auth_ssl_ocsp</li><li>_sys_auth_tacacs</li></ul>
Enabled	Available				
	<ul style="list-style-type: none"><li>_sys_auth_ldap</li><li>_sys_auth_radius</li><li>_sys_auth_ssl_cc_ldap</li><li>_sys_auth_ssl_ocsp</li><li>_sys_auth_tacacs</li></ul>				
HTTP Class Profiles	<table border="1"><thead><tr><th>Enabled</th><th>Available</th></tr></thead><tbody><tr><td></td><td><ul style="list-style-type: none"><li>httpclass</li></ul></td></tr></tbody></table>	Enabled	Available		<ul style="list-style-type: none"><li>httpclass</li></ul>
Enabled	Available				
	<ul style="list-style-type: none"><li>httpclass</li></ul>				
Default Pool	<input type="text" value="wts_pool"/>				
Default Persistence Profile	<input type="text" value="wts_rdp"/>				
Fallback Persistence Profile	<input type="text" value="None"/>				

Cancel Repeat Finished

*Figure 6 Resources section of the add virtual server page*

10. Click the **Finished** button.

## 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

### Saving up and restoring the BIG-IP 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.