



Deploying the BIG-IP LTM with Microsoft Windows Server 2008 R2 Remote Desktop Services



Deploying the BIG-IP LTM with Microsoft Windows Server 2008 R2 Remote Desktop Services

Welcome to the BIG-IP - Microsoft® Windows® Server 2008 R2 Remote Desktop Services deployment guides (formerly Windows Terminal Services). This guide gives you step-by-step configuration procedures for configuring the BIG-IP LTM (Local Traffic Manager) system for directing traffic and maintaining persistence to Microsoft Remote Desktop Services.

Remote Desktop Services in Windows Server 2008 R2 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 has 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 Gateway and Web Access roles in Remote Desktop Services.

For more information on Microsoft Windows Server 2008 R2, including Windows Remote Desktop Services, see <http://technet.microsoft.com/en-us/library/dd647502%28WS.10%29.aspx>

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

This Deployment Guide is broken up into three sections:

- *Scenario 1: BIG-IP LTM for Remote Desktop Access with RD Session Host and RD Connection Broker*, on page 1-4
- *Scenario 2: Adding Remote Desktop Gateway to the BIG-IP LTM configuration*, on page 1-11
- *Scenario 3: Adding Remote Desktop Web Access to the BIG-IP LTM configuration*, on page 1-17

Prerequisites and configuration notes

The following are general prerequisites for this deployment, each section has its own prerequisites:

- ◆ The BIG-IP LTM system should be running version 10.1 or later. Other than minor interface differences, the configuration described in this guide should apply to BIG-IP version 9.4.2 and later.
- ◆ You must also be using Windows Server 2008 R2 Remote Desktop Services. If you are using a previous version of the BIG-IP LTM system or Remote Desktop/Terminal Services, see the *Deployment Guide* index.
- ◆ You should be familiar with both the BIG-IP LTM system and Windows Server 2008 R2 Remote Desktop Services. For more information on configuring these products, consult the appropriate documentation.
- ◆ BIG-IP LTM offers the ability to mix IPv4 and IPv6 addressing; for instance, you might want to use IPv6 addressing on your internal networks even though connections from clients on the Internet use IPv4.

We show one example of this type of configuration later in this document.

For versions of the BIG-IP LTM prior to 10.0, you may need to license the IPv6 gateway. Talk to your sales representative for details.

- ◆ Although our examples and diagrams show external users connecting to the BIG-IP in a *routed* configuration, the steps described in this document are equally valid for a *one-armed* configuration, and both topologies may be used simultaneously.
- ◆ The third-party Web site information in this guide is provided to help you find the technical information you need. The URLs are subject to change without notice.

Configuration examples

This deployment guide details three configuration scenarios:

- ◆ ***Scenario 1: BIG-IP LTM for Remote Desktop Access with RD Session Host and RD Connection Broker***, on page 1-4
In this scenario, we configure a BIG-IP LTM for use with Remote Desktop Access. Users connect through the BIG-IP LTM to an RD Session Host server farm using the Remote Desktop Protocol (RDP), with an RD Connection Broker server managing persistence. The BIG-IP LTM provides advanced load balancing to farm members, while honoring RD Connection Broker routing tokens. This is the path labeled **1** in the following diagram.
- ◆ ***Scenario 2: Adding Remote Desktop Gateway to the BIG-IP LTM configuration***, on page 1-11
In this scenario, we extend and modify the deployment to add a farm of RD Gateway Servers. While still using the Remote Desktop Connection client, users' RDP sessions are now encapsulated in HTTPS, which is more likely to be allowed through firewalls. When the HTTPS sessions arrive at the BIG-IP, they are decrypted and passed to a farm of RD Gateway servers using HTTP. The RD Gateway Servers remove the HTTP, and forward the RDP sessions back to the BIG-IP LTM, where we've moved the RDP virtual server to the internal (private) network. BIG-IP LTM distributes those connections to the same RD Session Host farm that was used in Example 1. This is the path labeled **2** in the following diagram.
- ◆ ***Scenario 3: Adding Remote Desktop Web Access to the BIG-IP LTM configuration***, on page 1-17
In this scenario, we extend the deployment again to include RD Web Access Servers and RemoteApp. Users browse to a web page via HTTPS; their sessions are decrypted on the BIG-IP LTM and passed to a farm of RD Web Access servers over HTTP. By selecting applications that have been published on that page, users initiate new connections to individual RemoteApp resources, while still using the BIG-IP LTM and RD Gateway Server farm to encapsulate their connection in HTTPS. This is the path labeled **3** in the following diagram.

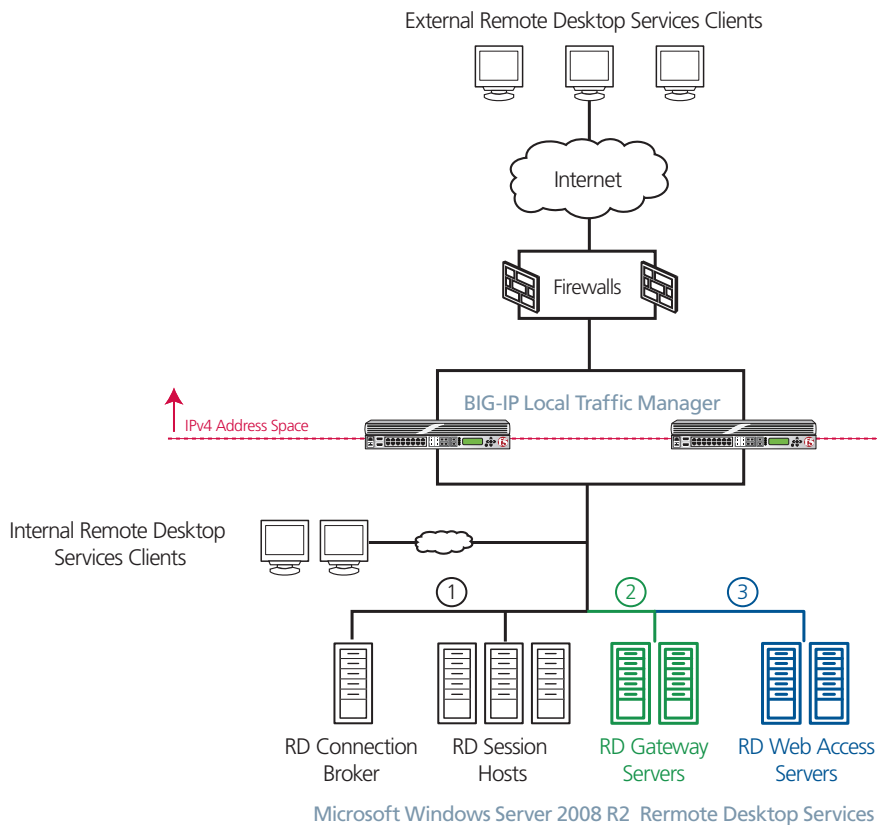


Figure 1 Logical configuration example, including all three deployment scenarios

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

Product versions and revision history

Product and versions tested for this deployment guide:

Product Tested	Version Tested
BIG-IP LTM	v10.1
Microsoft Remote Desktop Services	Microsoft Windows Server 2008 R2 Remote Desktop Services

Document Version	Description
1.0	New deployment guide

Scenario I: BIG-IP LTM for Remote Desktop Access with RD Session Host and RD Connection Broker

In this scenario, we show you how to configure a BIG-IP LTM for use with Remote Desktop Access. For a description of this scenario, see *Configuration examples*, on page 2.

Prerequisites and configuration notes

The following are prerequisites and notes specific to this scenario. These notes apply to the Remote Desktop Services configuration.

- ◆ Install the Remote Desktop Session Host role on at least one server; for load balancing connections, you need at least two servers. See the Microsoft document **Installing Remote Desktop Session Host Step-by-Step guide** available at:
[http://technet.microsoft.com/en-us/library/dd883275\(WS.10\).aspx](http://technet.microsoft.com/en-us/library/dd883275(WS.10).aspx).
- ◆ Install the Remote Desktop Connection Broker role on at least one server according to the Microsoft document:
technet.microsoft.com/en-us/library/dd883258%28WS.10%29.aspx.
Make sure the servers are part of a RD Connection Broker farm.
- ◆ The following are requirements for the RD Connection Broker farm:
 - Members should match those in the BIG-IP LTM pool.
 - Members should **not** participate in Connection Broker load balancing.
 - Use token redirection.
 - RD Connection Broker defined (host with Session Broker role installed).
 - Farm name must be the DNS name that will be associated with the BIG-IP LTM virtual server IP address (see Figure 2).

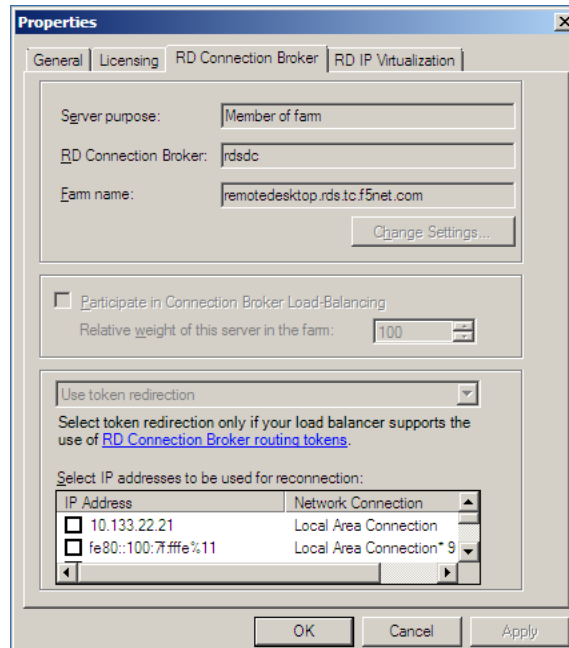


Figure 2 Configuring the TS Session Broker properties

Configuring the BIG-IP LTM

The following table contains the BIG-IP LTM configuration objects necessary for this scenario.

Remote Desktop Service	Monitor	Pool Member Port	Profiles	VIP Port/Notes
Remote Desktop Access with RD Session Host and RD Connection Broker	TCP	3389 Load Balancing Method: Least Connections (member)	- TCP (LAN or WAN optimized parent, depending on where clients are located) - Persistence: Type= Microsoft® Remote Desktop	- 3389 - Set SNAT Pool to Automap

Configuring the TCP health monitor

For this configuration, we create a simple TCP 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 configure the TCP 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 **RD-SessionHost-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. In our example, we use an **Interval** of **30** and a **Timeout** of **91**.
6. In the **Send String** and **Receive Rule** boxes, you can add a Send String and Receive Rule specific to the device being checked.
7. All other fields are optional, configure as applicable to your implementation.
8. Click **Finished**.

Creating the pool

The next task is to create a load balancing pool on the BIG-IP system for the RD Session Host servers. In our example, we use IPv6 addresses for the pool members. These may be IPv4 addresses in your configuration.

To create a new pool for the RD Session Host servers

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. From the **Configuration** list, select **Advanced**.
4. In the **Name** box, type a name for the pool. We use **RD-SessionHost-pool**.
5. In the **Health Monitors** section, select the name of the monitor you created in the *Configuring the TCP health monitor* section, and click the Add (<<) button. In our example, we select **RDS-tcp**.
6. *Optional:* In the **Slow Ramp Time** box, type **300** (see Figure 3).
Because we are using the Least Connections load balancing method, we set the Slow Ramp Time in order to ensure that if a pool member becomes available after maintenance or a new member is added, the BIG-IP does not send all new connections to that member (a newly available member always has the least number of connections).
7. From the **Load Balancing Method** list, choose your preferred load balancing method (different load balancing methods may yield optimal results for a particular network). In our example, we select **Least Connections (member)**.
8. In the New Members section, make sure the **New Address** option button is selected.

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

Configuration: **Advanced**

Name	RD-SessionHost-pool	
Health Monitors	<div>Active</div> <div>RD-SessionHost-tcp</div>	<div>Available</div> <div>gateway_icmp http https https_443 inband</div>
Availability Requirement	All	Health Monitor(s)
Allow SNAT	Yes	
Allow NAT	Yes	
Action On Service Down	None	
Slow Ramp Time	300 seconds	

Figure 3 Pool configuration options

9. In the **Address** box, add the first server to the pool. In our example, we type **2001:db1::a** (when the BIG-IP system creates this node, it automatically expands IPv6 address to add implied zeros. In this case, the node is added as 2001:db1:0:0:0:0:a).
10. In the **Service Port** box, type **3389**.
11. Click the **Add** button to add the member to the list.
12. Repeat steps 9-11 for each RD Session Host server. In our example, we repeat these steps for **2001:db1::b** and **2001:db1::c**.
13. Click the **Finished** button.

Resources

Load Balancing Method	Least Connections (member)	
Priority Group Activation	Disabled	
New Members	<input checked="" type="radio"/> New Address <input type="radio"/> Node List	
	Address:	2001:db1::c
	Service Port:	3389 Select...
	<div>Add</div> <div> R:1 P:0 C:0 2001:db1::a .3389 R:1 P:0 C:0 2001:db1::b .3389 R:1 P:0 C:0 2001:db1::c .3389 </div> <div>Edit Delete</div>	
<div>Cancel Repeat Finished</div>		

Figure 4 Pool Resources

Creating the profiles

The next task is to create the 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. For this scenario, we create two profiles, a TCP profile and a persistence profile.

Creating the TCP profile

The first profile is a TCP profile. The parent TCP profile you use depends on where the clients are located. If most clients are on the LAN, use the **tcp-lan-optimized** parent profile. If most clients are coming over the WAN, use the **tcp-wan-optimized** parent.

To create the 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 **RD-SessionHost-tcp**.
5. From the **Parent Profile** list, select either **tcp-lan-optimized** or **tcp-wan-optimized**, depending on where your clients are located.
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 persistence profile

The other profile we create in this scenario is a persistence profile. The BIG-IP LTM contains a persistence profile specifically designed for Microsoft Remote Desktop.

To create the 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**.
3. 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 **RD-SessionHost-persistence**.
5. From the **Persistence Type** list, select **Microsoft® Remote Desktop**.
The configuration options for Microsoft Remote Desktop appear. Make sure the Parent Profile is set to **msrdp**.

6. Modify any of the options as applicable for your network.
7. Click the **Finished** button.

Creating the virtual server

The final task in this scenario is to create the virtual server that uses the profiles and pool you created in the preceding procedures.

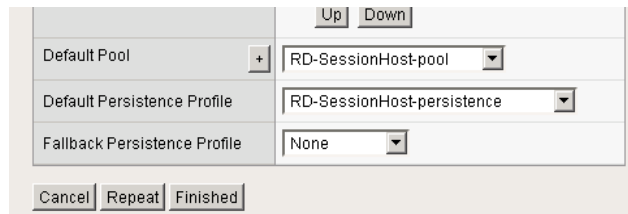
To create the virtual server

1. On the Main tab, expand **Local Traffic**, and then click **Virtual Servers**.
2. 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 **RD-SessionHost-vs**.
4. In the **Destination** section, click the **Host** button.
5. In the **Address** box, type the IP address of this virtual server. In our example, we use **192.0.2.10**.
6. In the **Service Port** box, type **3389**.
7. From the Configuration list, select **Advanced**.
8. From the **Protocol Profile (Client)** list, select the name of the profile you created in *Creating the TCP profile*, on page 8. In our example, we select **RD-SessionHost-tcp**.
If you did not create a WAN optimized tcp profile, leave this at the default.
9. From the **Protocol Profile (Server)** list, if you created a LAN optimized TCP profile in *Creating the TCP profile*, on page 8, select the name of the profile. If you did not, leave this at the default.

Local Traffic >> Virtual Servers: Virtual Server List >> New Virtual Server...	
General Properties	
Name	RD-SessionHost-vs
Destination	Type: <input checked="" type="radio"/> Host <input type="radio"/> Network Address: 192.0.2.10
Service Port	3389 Other: <input type="text"/>
State	Enabled
Configuration: Advanced	
Type	Standard
Protocol	TCP
Protocol Profile (Client)	RD-SessionHost-tcp
Protocol Profile (Server)	All Client Profiles

Figure 5 Virtual server configuration

10. From the **SNAT Pool** list, select **Automap**.
11. In the Resources section, from the **Default Pool** list, select the pool you created in *Creating the pool*, on page 6. In our example, we select **RD-SessionHost-pool**.
12. From the **Default Persistence Profile** list, select the persistence profile you created in *Creating the persistence profile*, on page 8. In our example, we select **RD-SessionHost-persistence**.
13. Click the **Finished** button.



The screenshot shows a configuration window for a virtual server. At the top right are 'Up' and 'Down' buttons. Below them is a table with three rows: 'Default Pool' with a '+' button and a dropdown menu showing 'RD-SessionHost-pool'; 'Default Persistence Profile' with a dropdown menu showing 'RD-SessionHost-persistence'; and 'Fallback Persistence Profile' with a dropdown menu showing 'None'. At the bottom are 'Cancel', 'Repeat', and 'Finished' buttons.

	Up	Down
Default Pool	+	RD-SessionHost-pool
Default Persistence Profile		RD-SessionHost-persistence
Fallback Persistence Profile		None

Cancel Repeat Finished

Figure 6 Resource section of the virtual server (condensed)

This completes the configuration for scenario 1.

Scenario 2: Adding Remote Desktop Gateway to the BIG-IP LTM configuration

The Remote Desktop Gateway allows authorized users to tunnel 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;
- Publication of a single name and address to the public networks, rather than one for each internal RD Session Host resource.

In the deployment described in scenario 1, users on the Internet connect to a BIG-IP virtual server for RD Session Host functionality over TCP port 3389. In typical configurations, the RD Session Host virtual server will therefore have a public IP address on an Internet-facing side of the BIG-IP LTM.

In the following scenario, however, where you introduce an RD Gateway server farm and corresponding BIG-IP virtual server, you may want to allow clients to connect only through an RD Gateway server farm using HTTPS. If that is the case, the BIG-IP RD Session Host virtual server can be moved to a “private” IP address on an internal network. The new RD Gateway virtual server you create must be on a public-facing IP address and accessible on TCP port 443.

Prerequisites and configuration notes

The following are prerequisites and notes specific to this scenario. These notes apply to the Remote Desktop Services configuration.

- ◆ Install the Remote Desktop Gateway role on at least one server; for load-balancing connections, you need at least two servers. See Deploying Remote Desktop Gateway Step-by-Step Guide at: technet.microsoft.com/en-us/library/dd983941%28WS.10%29.aspx
- ◆ Install the Remote Desktop Session Host role, as described in Scenario 1.
- ◆ Install the Remote Desktop Connection Broker role on at least one server, as described in Scenario 1.
- ◆ Create an RD Gateway Server Farm:
 - Add all members of farm (must match those in LTM pool)
 - Enable HTTPS - HTTP Bridging
 - SSL Certificate: any setting will work, the LTM does SSL processing

- ◆ Each user's Remote Desktop Connection client needs to be configured to use an RD Gateway Server. The configured Server Name must correspond to the fully-qualified DNS name that is associated with the Client SSL profile that you create on the BIG-IP LTM.

Additionally, the certificate associated with that name and profile must be trusted by the client computer, and the client computer must be able to resolve the DNS name to the IP address assigned to the BIG-IP virtual server.

Instructions for the various methods of client configuration can be found in the following Microsoft TechNet article:

(<http://technet.microsoft.com/en-us/library/cc772479.aspx>)

In our example, we show a manually configured Remote Desktop Connection client.

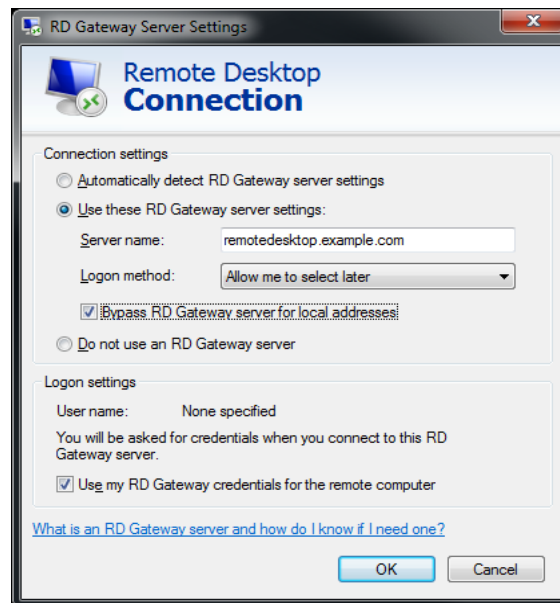


Figure 7 RD Gateway Server settings

In the following screenshots, we show an example of a RD Gateway server that has been properly configured to participate in a RD Gateway server farm. In Figure 8, you can see that **SSL Bridging** has been enabled. Figure 9 shows that two members have been added to the farm.

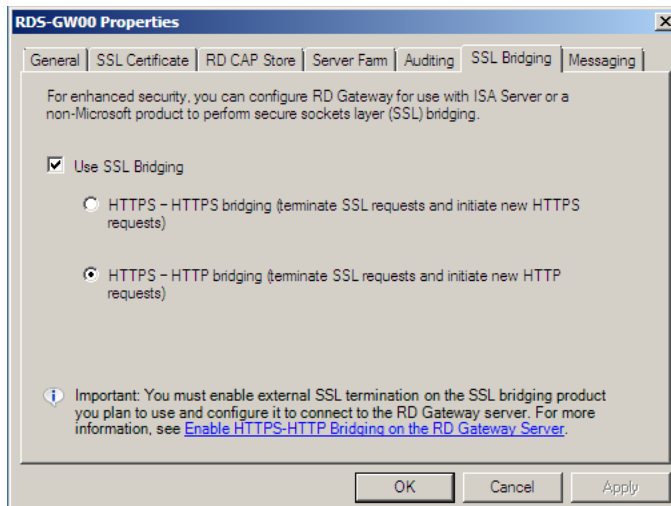


Figure 8 Configuring HTTPS-HTTP bridging on the TS Gateway server

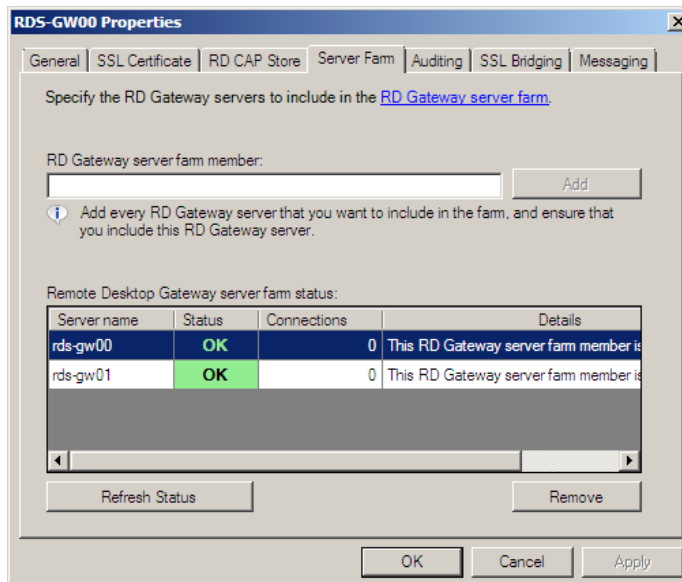


Figure 9 Configuring the Server Farm properties

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

Configuring the BIG-IP LTM

The following table contains the BIG-IP LTM configuration objects necessary for this scenario.

Remote Desktop Service	Monitor	Pool Port/Notes	Profiles	VIP Port/Notes
<i>Remote Desktop Gateway</i>	TCP	80 Load Balancing Method: Least Connections (member)	<ul style="list-style-type: none"> - TCP (LAN or WAN optimized parent, depending on where the majority of your clients originate) - HTTP: basic http parent - ClientSSL: use certificate with DNS name you want to use for the virtual server - Persistence: Universal parent Timeout: 3600 (as applicable) Use iRule (below) 	<ul style="list-style-type: none"> - 443 - Set SNAT Pool to Automap

Creating the TCP health monitor

To configure the TCP health monitor, use the procedure *Configuring the TCP health monitor*, on page 5. Give the monitor a unique name, such as **RD-Gateway-tcp**.

Creating the pool

To configure the load balancing pool, use the procedure *Creating the pool*, on page 6. Give the pool a unique name, such as **RD-Gateway-pool**. Use the appropriate RD Desktop Gateway IP addresses. The Service Port is **80**. Associate the monitor you just created with the pool.

Creating the iRule

The next object we configure is an iRule that is used for persistence. This iRule is necessary because the Microsoft Remote Desktop Connection client does not support HTTP cookies, so the BIG-IP LTM uses this iRule to base persistence on other information in the HTTP headers. 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 persistence iRule

1. On the Main tab, expand **Local Traffic**, and then click **iRules**.
2. Click the **Create** button. The New iRule screen opens.

-
3. In the **Name** box, type a name for your iRule. In our example, we use **RD-Gateway-persist-irule**.
 4. In the **Definition** section, copy and paste the following iRule, omitting the line numbers:

```
1  when HTTP_REQUEST {  
2      if { [HTTP::header exists "Authorization"] } {  
3          persist uie [HTTP::header "Authorization"]  
4      }  
5  }
```

5. Click the **Finished** button.

Creating the profiles

For this scenario, we create TCP, HTTP, persistence and SSL profiles.

For the SSL profile, we assume you have already acquired an SSL certificate and installed it on the BIG-IP LTM. For specific information, see the online help or the BIG-IP LTM documentation, available on [Ask F5](#).

Creating the TCP profile

To create the TCP profile, use the procedure *Creating the TCP profile*, on page 8. Use a unique name; all other settings are optional.

Creating the HTTP profile

The next profile is an HTTP profile. This should be based on the simple HTTP parent profile and not one of the optimized profile types.

To create a new HTTP profile

1. On the Main tab, expand **Local Traffic**, click **Profiles**, and then click the **Create** button.
2. In the **Name** box, type a name. In our example, we type **RD-Gateway-http**.
3. From the **Parent Profile** list, select **http**.
4. Click the **Finished** button.

Creating the persistence profile

Next we create the persistence profile that uses the iRule you created earlier.

To create a new persistence profile

1. On the Main tab, expand **Local Traffic**, click **Profiles**, and then, on the Menu bar, click **Persistence**.

2. Click the **Create** button.
3. In the **Name** box, type a name. In our example, we type **RD-Gateway-persist**.
4. From the **Persistence Type** list, select **Universal**.
5. In the **iRule** row, check the **Custom** box. From the list, select the iRule you created in *Creating the iRule*, on page 14. In our example, we select **RD-Gateway-persist-irule**.
6. Click the **Finished** button.

Creating the Client SSL profile

The final profile is the Client SSL profile. This profile contains the SSL certificate and Key information for offloading the SSL traffic. If you have not yet installed a certificate on the BIG-IP LTM, you must do so before creating this profile. See the online help or BIG-IP documentation for specific instructions.

To create a new Client SSL profile

1. On the Main tab, expand **Local Traffic**, click **Profiles**, and then, on the Menu bar, from the **SSL** menu, click **Client**.
2. Click the **Create** button. The New Client SSL Profile screen opens.
3. In the **Name** box, type a name. We type **RD-Gateway-clientssl**.
4. In the Configuration section, click a check in the **Certificate** and **Key** Custom boxes.
5. From the **Certificate** list, select the name of the Certificate you imported.
6. From the **Key** list, select the key you imported.
7. Click the **Finished** button.

Creating the virtual server

The final task in this scenario is to create the virtual server. To create the virtual server, use the procedure *Creating the virtual server*, on page 9, with the following changes:

- In step 3, use a unique name, such as **RD-Gateway-vs**
- In step 5, use the appropriate IP address.
- In step 6, use port **443**.
- Select the profiles and pool you created in the procedures in this section.
- After step 9, from the **HTTP Profile** list, select the profile you created in *Creating the HTTP profile*, on page 15.
From the **SSL Profile (Client)** list, select the profile you created in *Creating the Client SSL profile*, on page 16.

Scenario 3: Adding Remote Desktop Web Access to the BIG-IP LTM configuration

In this section, we configure the BIG-IP LTM for the RD Web Access server component. The Web Access role allows authorized users to connect to a web site that presents pre-configured icons for access to either individual applications (RemoteApp) or Remote Desktops on RD Session Host farms. 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.

Prerequisites

- ◆ Install the Remote Desktop Web Access role on at least one server; for load-balancing connections, you will need at least two servers. See the Microsoft document here: technet.microsoft.com/en-us/library/dd883258%28WS.10%29.aspx (Installing Remote Desktop Web Access with Remote Desktop Connection Host Step-by-Step Guide).
- ◆ Install the Remote Desktop Session Host role, as described previously.
- ◆ Install the Remote Desktop Connection Broker role on at least one server, as described previously.
- ◆ Clear the **Require SSL** box in Internet Information Services manager for the RDWeb virtual directory and its sub-directories Feed, FeedLogin, and Pages (see Figure 11).
- ◆ **Important:** You must complete the prerequisites in this list **before** you attempt to configure a RemoteApp source that corresponds to a farm of Session Host server that is load balanced by BIG-IP LTM. Otherwise, you will be unsuccessful.
- ◆ The DNS name that will be used by LTM virtual must be resolvable by Web Access servers; choose **One or more RemoteApp sources** during configuration (the virtual server must already exist) and use the DNS Name (see Figure 10).

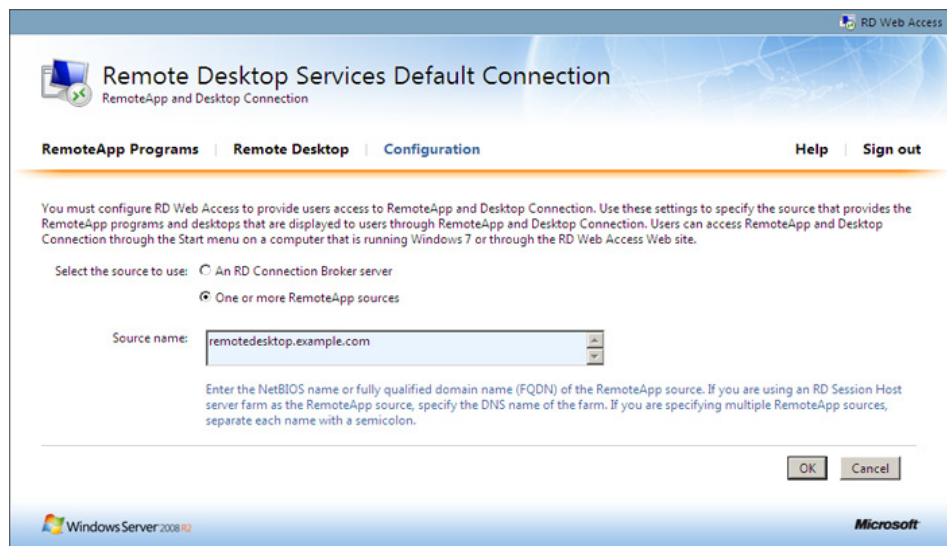
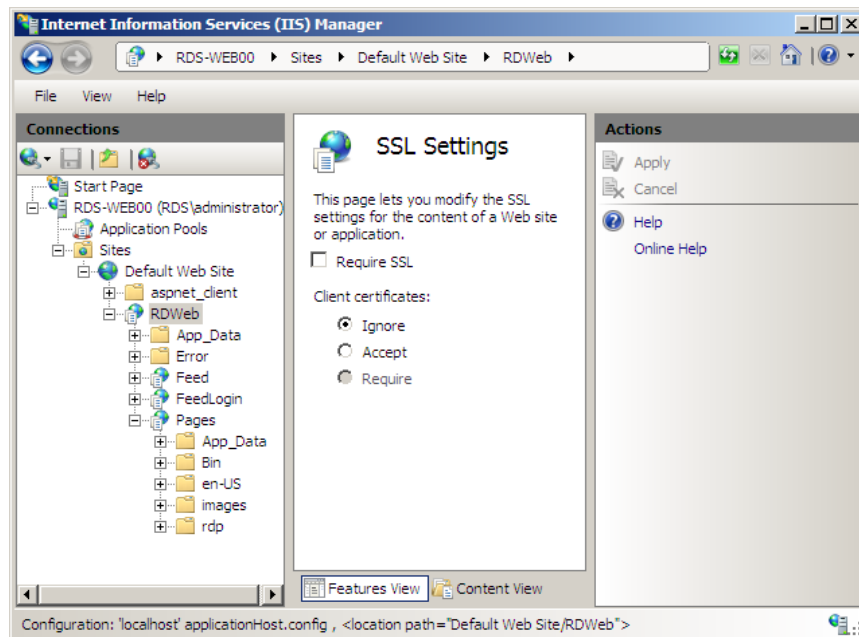


Figure 10 Remote Desktop Services default connection page



Configuring the BIG-IP LTM

The following table contains the BIG-IP LTM configuration objects necessary for this scenario.

Remote Desktop Service	Monitor	Pool Port/Notes	Profiles	VIP Port/Notes
<i>Remote Desktop Web Access 443</i>	TCP	80 (all RD Web Access Servers) Load Balancing Method: Least Connections (member)	<ul style="list-style-type: none">- TCP (LAN or WAN optimized parent, depending on where the majority of your clients originate)- HTTP: http-lan-optimized-caching parent with Redirect Rewrite set to All.- ClientSSL: use certificate with DNS name you want to use for the virtual server- Persistence: Cookie	<ul style="list-style-type: none">- 443- Set SNAT Pool to Automap
<i>Remote Desktop Web Access 135</i>	TCP	135 (all RD Session Host servers) Load Balancing Method: Least Connections (member)	TCP: tcp-lan-optimized parent	<ul style="list-style-type: none">- 135- Set SNAT Pool to Automap

Creating the TCP health monitors

For RD Web Access, we create two TCP health monitors. Use the procedure *Configuring the TCP health monitor*, on page 5. Give each monitor a unique name, such as **RD-WebAccess443-tcp** and **RD-WebAccess135-tcp** (Note: the port numbers in our example names are just to differentiate between the two monitors. In our example, these are both simple TCP monitors).

Creating the pools

In this section, we create two pools, one that contains the RD Web Access servers, and one that contains the RD Session Host Servers on port 135.

- ◆ For the RD Web Access server pool, use the procedure *Creating the pool*, on page 6. Give the pool a unique name, such as **RD-WebAccess-80-pool**. Use the appropriate RD Web Access IP addresses. The Service Port is **80**. Associate the monitor you just created with the pool.
- ◆ For the RD Session Hosts Server on port 135, use the procedure *Creating the pool*, on page 6. Give the pool a unique name, such as **RD-WebAccess-135-pool**. Use the appropriate RD Web Access IP addresses. The Service Port is **135**. Associate the monitor you just created with the pool.

Creating the profiles

The next step is to create the profiles.

- ◆ For the RD Web Access servers, create the following profiles
 - TCP profile: Use *Creating the TCP profile*, on page 8. Give the profile a unique name, all other settings are optional.
 - HTTP profile: Use *Creating the HTTP profile*, on page 15 with the following changes:
 - Use a unique name.
 - From the **Parent Profile** list, select **http-lan-optimized-caching**.
 - In the **Redirect Rewrite** row, check the **Custom** box, and then select **All** from the list.
 - Client SSL profile. Use *Creating the Client SSL profile*, on page 16. Use a unique name and choose a certificate and key that are correct for the DNS name associated with this BIG-IP virtual server.
 - Persistence Profile. Use *Creating the persistence profile*, on page 15 but from the **Parent Profile** list, select **Cookie**. All other settings are optional.
- ◆ For the RD Session Hosts Server on port 135, only create a TCP profile using *Creating the TCP profile*, on page 8. Select the tcp-lan-optimized parent, and give the profile a unique name, all other settings are optional.

Creating the virtual servers

The final task in this scenario is to create the virtual servers. To create the virtual server, use the procedure *Creating the virtual server*, on page 16, with the following changes:

- ◆ For the RD Web Access virtual server:
 - In step 3, use a unique name, such as **RD-WebAccess-443-vs**
 - In step 5, use the appropriate IP address.
 - In step 6, use port **443**.
 - Select the profiles and pool you created in the procedures in this section.
- ◆ For the RD Session Hosts Server on port 135 virtual server:
 - In step 3, use a unique name, such as **RD-WebAccess-135-vs**
 - In step 5, use the appropriate IP address.
 - In step 6, use port **135**.
 - Select the profiles and pool you created in the procedures in this section.

This completes the BIG-IP LTM configuration for Microsoft Remote Desktop Services.

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