Deployment Guide

Deploying F5 with Microsoft Remote Desktop Services

IMPORTANT: This guide has been archived. There are two newer deployment guides and downloadable iApp templates available for Remote Desktop Services, one for the Remote Desktop Gateway Servers, and one for Remote Desktop Session Host. See downloads.f5.com for the iApp templates, or the Deployment Guide index at *https://f5.com/solutions/deployment-guides/tag/microsoft* to find the associated deployment guides.

Welcome to the F5 deployment guide for Microsoft® Remote Desktop Services included in Windows® Server 2012 and Windows Server 2008 R2. This document provides guidance on configuring the BIG-IP Local Traffic Manager (LTM) and Access Policy Manager (APM) for directing traffic and maintaining persistence to Microsoft Remote Desktop Services.

Remote Desktop Services enables users to remotely access full Windows desktops, or individual Windows-based applications, on Remote Desktop Session Host computers. In an environment using BIG-IP LTM system, a farm of Remote Desktop Session Host servers has incoming connections distributed in a balanced manner across the members of the farm. Additionally, BIG-IP LTM can offload SSL processing for the Gateway role in Remote Desktop Services.

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

Visit the Microsoft page of F5's online developer community, DevCentral, for Microsoft forums, solutions, blogs and more: *http://devcentral.f5.com/Microsoft/*.

Products and versions

Product	Version
BIG-IP LTM	10.1 and later in the 10.x branch, 11.0, 11.0.1, 11.1, 11.2, 11.3, 11.4. 11.4.1, 11.5, 11.5.1, 11.6
BIG-IP APM	11.0, 11.0.1, 11.1, 11.2, 11.3, 11.4, 11.4.1. 11.5, 11.5.1, 11.6
Microsoft Windows Server Remote Desktop Services	2012 R2, 2012, 2008 R2
Deployment Guide version	3.7 (see *Document Revision History on page 29*)

Important: *Make sure you are using the most recent version of this deployment guide, available at http://www.f5.com/pdf/deployment-guides/f5-microsoft-remote-desktop-services-dg.pdf*

Microsoft Partner Network

Contents

Prerequisites and configuration notes

- The BIG-IP LTM system must be running version 10.1 or later. We recommend using BIG-IP version 11.4 or later. For more information on the BIG-IP system, see *http://www.f5.com/products/bigip/*.
- You must be using Windows Server 2008 R2 or 2012 or 2012 R2 Remote Desktop Services. If you are using a previous version see the Deployment Guide index at: *http://www.f5.com/solutions/resources/deployment-guides.html*.
- For more information on Microsoft Windows Server, including Windows Remote Desktop Services, see one of the following links:
  - Windows Server 2012: *technet.microsoft.com/library/hh831447*
  - Windows Server 2008 R2: *technet.microsoft.com/en-us/library/dd647502%28WS.10%29.aspx*
- You should be familiar with both the BIG-IP LTM system and Windows Server Remote Desktop (RD) Services. For more information on configuring these products, consult the appropriate documentation.
- The 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.
- Although our examples and diagrams show external users connecting to the BIG-IP system 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.
- Be sure to see *Appendix A: Configuring WMI monitoring of the RDS servers on page 24* and *Appendix B: Using X-Forwarded-For to log the client IP address in IIS 7.0, 7.5, and 8 (optional) on page 26* for optional configuration procedures.
- There is now an iApp template developed by F5 for Remote Desktop Session Host, which greatly simplifies the configuration. For details, see *https://devcentral.f5.com/wiki/iApp.Microsoft-Remote-Desktop-Session-Host-iApp.ashx.*

Configuration example

This deployment guide details four configuration scenarios:

- *Scenario 1: Configuring the BIG-IP LTM for Remote Desktop Access with RD Session Host on page 5*
  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: Configuring the BIG-IP LTM for Remote Desktop Access with RD Gateway on page 8*
  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 to the destination Remote Desktop server specified by the client. This is the path labeled 2 in the following diagram. Optionally, you can deploy a virtual server to act as a reverse proxy in a perimeter or DMZ network. This virtual server forwards Remote Desktop Gateway HTTP traffic to a virtual server on the internal BIG-IP, which then forwards the RDP sessions to the destination Remote Desktop server. The reverse proxy virtual server is secured by an iRule that allows clients to connect to only the published Remote Desktop Services. Publishing Remote Desktop Gateway in this manner simplifies deployment and precludes exposing required services in the DMZ network.
- *Scenario 3: Configuring the BIG-IP LTM for the Remote Desktop Connection Broker service on page 14*
  If you have configured high availability for RD Connection Broker (available in Windows Server 2012 and 2012 R2 only), BIG-IP LTM load balances requests from the Remote Desktop Gateway servers to the Connection Broker service between all members of the RD Connection Broker farm.
- *Scenario 4: Adding Remote Desktop Web Access to BIG-IP LTM on page 16*
  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.

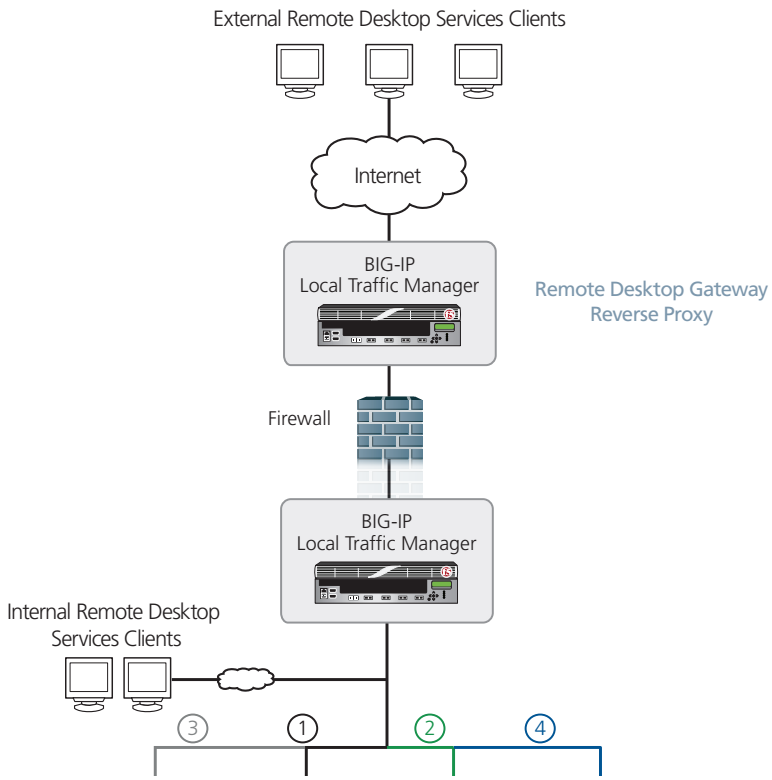

Figure 1: *Logical configuration example*

- *Scenario 5: Publishing Remote Desktop Resources using BIG-IP APM on page 19*
  In this scenario, the BIG-IP Access Policy Manager allows you to securely publish Remote Desktop connections and programs, which users can access using links on an APM Webtop. This can eliminate the need to locate a Remote Desktop Web Access server in the DMZ or perimeter network.

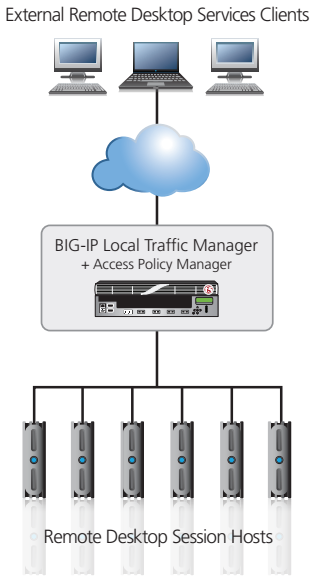

Figure 2: *BIG-IP APM logical configuration example*

Scenario 1: Configuring the BIG-IP LTM for Remote Desktop Access with RD Session Host

In this scenario, we show you how to configure the BIG-IP LTM for use with Remote Desktop Access and Remote Desktop Connection Broker. For a description of this scenario, see *Configuration example on page 3*.

There is now an iApp template developed by F5 for this scenario, which greatly simplifies the configuration. For details, see *https://devcentral.f5.com/wiki/iApp.Microsoft-Remote-Desktop-Session-Host-iApp.ashx.*

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* (for Windows Server 2008 R2).
- Install the Remote Desktop Connection Broker role on at least one server according to the Microsoft document: *http://technet.microsoft.com/en-us/library/dd883258%28WS.10%29.aspx* (for Windows Server 2008 R2). Make sure the servers are part of a RD Connection Broker farm.
- The following are requirements for the RD Connection Broker farm:
  - RD Connection Broker role is installed
  - Members should not participate in Connection Broker load balancing (Windows 2008 R2).
  - Members should use token redirection.
  - The farm may be configured in standard or high availability mode (Windows 2012 or 2012 R2 only). See *Scenario 3: Configuring the BIG-IP LTM for the Remote Desktop Connection Broker service on page 14* for more information.

Configuration table for scenario 1

The table on the following page contains a list of BIG-IP LTM configuration objects along with any non-default settings you should configure as a part of this deployment scenario. Unless otherwise specified, settings not mentioned in the table can be configured as applicable for your configuration. For specific instructions on configuring individual objects, see the online help or product manuals.

BIG-IP LTM Object	Non-default settings/Notes	
Health Monitor[1] (*Main tab-->Local Traffic -->Monitors*)	***Name***	Type a unique name
	Type	**TCP**
	Interval	**30** (recommended)
	Timeout	**91** (recommended)
	Send String[1] *(use the string for your version of Windows Server*	**Window Server 2012 R2**
		\x03\x00\x00\x13\x0E\xE0\x00\x00\x00\x00\x00\x01\x00\x08\x00\x0b\x00\x00\x00
		Window Server 2012, 2008 R2
		\x03\x00\x00\x13\x0E\xE0\x00\x00\x00\x00\x00\x01\x00\x08\x00\x03\x00\x00\x00
	Receive String[1] *(use the string for your version of Windows Server)*	**Window Server 2012 R2**
		\x03\x00\x00\x13\x0E\xD0\x00\x00\x12\x34\x00\x02\x0f\x08\x00\x08\x00\x00\x00
		Window Server 2012
		\x03\x00\x00\x13\x0E\xD0\x00\x00\x12\x34\x00\x02\x07\x08\x00\x02\x00\x00\x00
		Window Server 2008 R2
		\x03\x00\x00\x13\x0E\xD0\x00\x00\x12\x34\x00\x02\x01\x08\x00\x02\x00\x00\x00

[1] If you are using BIG-IP version 11.5.x, see *Troubleshooting on page 23*

BIG-IP LTM Object	Non-default settings/Notes		
Pool (*Main tab-->Local Traffic -->Pools*)	***Name***	Type a unique name	
	Health Monitor	Select the monitor you created above	
	Slow Ramp Time[1]	**300**	
	Load Balancing Method	Choose a load balancing method. We recommend **Least Connections (Member)**	
	Address	Type the IP Address of the RD Session Host nodes. This can be an IPv4 or IPv6 address.	
	Service Port	**3389** Click **Add**, and repeat Address and Port for all nodes	
Profiles (*Main tab-->Local Traffic -->Profiles*)	***TCP*** (*Profiles-->Protocol*)	Name	Type a unique name
		Parent Profile	Use **tcp-wan-optimized** or **tcp-lan-optimized** depending on where your clients are located.
		Nagle's Algorithm	If you selected *tcp-wan-optimized*: Clear the **Nagle's Algorithm** box to disable Nagle's Algorithm.
	Persistence (*Profiles-->Persistence)*	Name	Type a unique name
		Persistence Type	**Microsoft® Remote Desktop**
		Has Session Directory	If you are using Remote Desktop Connection Broker, check the **Has Session Directory** box.
Virtual Server (*Main tab-->Local Traffic -->Virtual Servers*)	***Name***	Type a unique name.	
	Address	Type the IP Address for the virtual server	
	Service Port	**3389**	
	Protocol Profile (client)[1]	Select the TCP profile you created above	
	Protocol Profile (server)[1]	Select the TCP profile you created above	
	SNAT Pool [2]	**Auto Map** (optional; see footnote [3])	
	Default Pool	Select the pool you created above	
	Default Persistence Profile	Select the Persistence profile you created	

[1] You must select **Advanced** from the **Configuration** list for these options to appear

[2] *If want to use SNAT, and you have a large deployment expecting more than 64,000 simultaneous connections, you must configure a SNAT Pool with an IP address for each 64,000 simultaneous connections you expect. See the BIG-IP documentation on configuring SNAT Pools.*

Supporting RemoteFX for Remote Desktop Session Host (optional)

If you are using Microsoft RemoteFX for Remote Desktop Services, use the following table to configure additional BIG-IP LTM objects for the Remote Desktop Session Host servers.

BIG-IP LTM Object	Non-default settings/Notes	
Health Monitor (*Main tab-->Local Traffic -->Monitors*)	**UDP Monitor**	
	Name	Type a unique name
	Type	**UDP**
	Interval	**30** (recommended)
	Timeout	**91** (recommended)
	Gateway ICMP Monitor	
	Name	Type a unique name
	Type	**Gateway ICMP**
	Interval	**30** (recommended)
	Timeout	**91** (recommended)

BIG-IP LTM Object	Non-default settings/Notes		
Pool (*Main tab-->Local Traffic -->Pools*)	***Name***	Type a unique name	
	Health Monitor	Select both monitors you created above (ensure *Availability Requirement* is set to **All** (the default)	
	Slow Ramp Time[1]	**300**	
	Load Balancing Method	Choose a load balancing method. We recommend **Least Connections (Member)**	
	Address	Type the IP Address of a Remote Desktop Session Host	
	Service Port	**3389** Click **Add**, and repeat Address and Port for all Remote Desktop Session Host devices	
Profiles (*Main tab-->Local Traffic -->Profiles*)	***Persistence*** (*Profiles-->Persistence)*	Name	Type a unique name
		Persistence Type	**Source Address Affinity**
		Match Across Services	**Enabled**
Virtual Servers (*Main tab-->Local Traffic -->Virtual Servers*)	**Remote Desktop Session Host virtual server**		
	Name	Type a unique name.	
	Address	Type the same IP Address you used for the Session Host virtual server in the table on the previous page.	
	Service Port	**3389**	
	SNAT Pool [2]	**Auto Map** (optional; see footnote [2])	
	Default Pool	Select the Remote Desktop Session Host pool you created above	
	Default Persistence Profile	Select the MSRDP Persistence profile you created using the guidance from the table on the previous page.	
	Fallback Persistence Profile	Select the Source Address persistence profile you created above.	

[1] *You must select **Advanced** from the **Configuration** list for these options to appear*
[2] *If want to use SNAT, and you have a large deployment expecting more than 64,000 simultaneous connections, you must configure a SNAT Pool with an IP address for each 64,000 simultaneous connections you expect. See the BIG-IP documentation on configuring SNAT Pools.*

Modifying the Session Host virtual server to use the Persistence profile you created

The final task is to modify the Session Host virtual server you configured (using the guidance on the previous page) to use the persistence profile you just created for RemoteFX as a fallback method.

To modify the virtual server

1. Expand **Local Traffic** and then click **Virtual Servers**.
2. Click the name of the TCP Session Host virtual server you created using the guidance from the table on page 5.
3. On the Menu bar, click **Resources**.
4. From the **Fallback Persistence Profile** list, select the name of the Source Address Affinity persistence profile you just created.
5. Click **Update**.

This completes the configuration for scenario 1.

Scenario 2: Configuring the BIG-IP LTM for Remote Desktop Access with RD Gateway

The Remote Desktop Gateway allows authorized users to tunnel RDP connections over HTTPS, using the standard Remote Desktop 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, you can create a BIG-IP virtual server on an internal network to receive Remote Desktop Gateway traffic forwarded from the perimeter or DMZ 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 the 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 and add all members of farm (must match those in the BIG-IP LTM pool). Enable HTTPS - HTTP Bridging. For the SSL Certificate any setting will work, the BIG-IP 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.

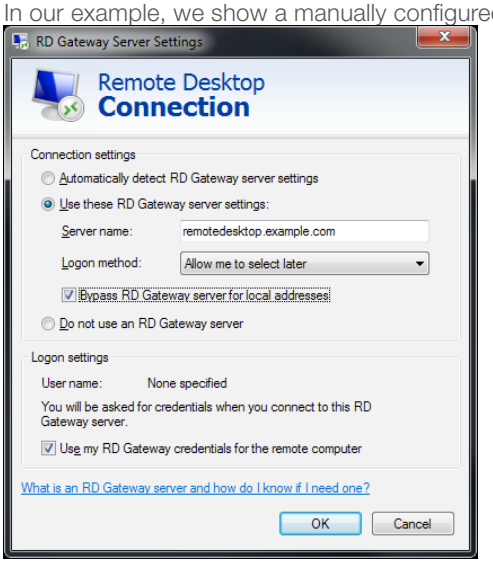

Figure 3: *RD Gateway Server settings*

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 3, you can see that SSL Bridging has been enabled. Figure 4 shows that two members have been added to the farm.

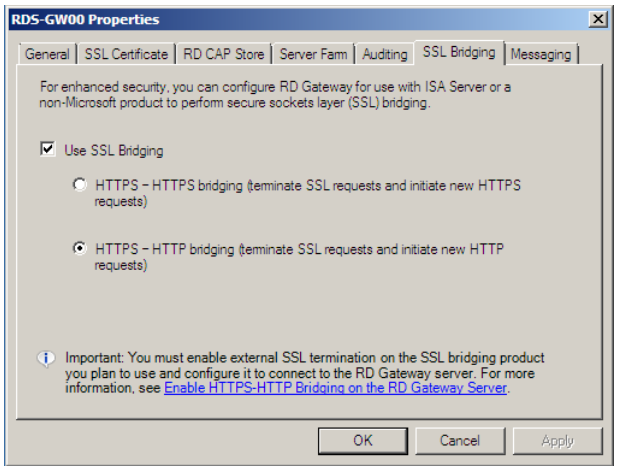

Figure 4: *Configuring HTTPS-HTTP bridging on the TS Gateway server*

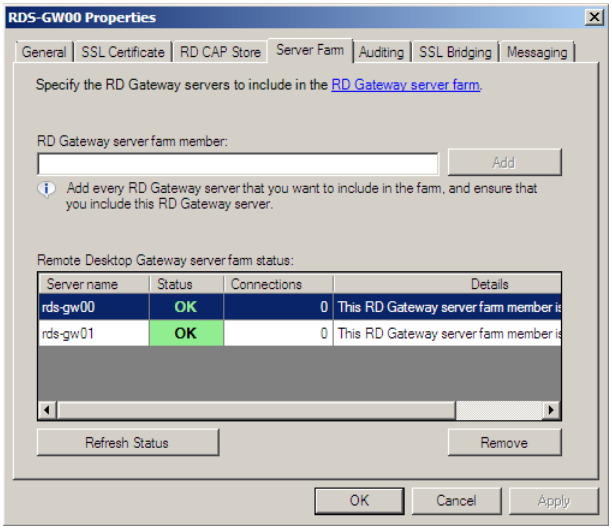

Figure 5: *Configuring the Server Farm properties*

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

Configuration table for scenario 2

The following table contains a list of BIG-IP LTM configuration objects along with any non-default settings you should configure as a part of this deployment scenario. Unless otherwise specified, settings not mentioned in the table can be configured as applicable for your configuration. For specific instructions on configuring individual objects, see the online help or product manuals.

If you plan on deploying Remote Desktop Web Access, and want to use the same IP address as Remote Desktop Gateway, see *Optional: Using a combined virtual server for Remote Desktop Gateway and Remote Desktop Web Access on page 22.*

Note

The health monitor requires a user account with permission to access the Remote Desktop Gateway. This is defined in the Client Access Policy on the RDG server. We recommend creating a user specifically for the health monitors.

BIG-IP LTM Object	Non-default settings/Notes		
Health Monitor (*Main tab-->Local Traffic -->Monitors*)	***Name***	Type a unique name	
	Type	**HTTP** (use **HTTPS** if configuring SSL Bridging)	
	Interval	**30** (recommended)	
	Timeout	**91** (recommended)	
	Send String	**RPC_IN_DATA /rpc/en-us/rpcproxy.dll HTTP/1.1\r\nHost: rdg.example.com** *(replace rdg.example.com with your host name)*	
	Receive String	**200 Success**	
	User Name	Type the user name of an account with RDG access.	
	Password	Type the associated password	
Pool (*Main tab-->Local Traffic -->Pools*)	***Name***	Type a unique name	
	Health Monitor	Select the monitor you created above	
	Slow Ramp Time[1]	**300**	
	Load Balancing Method	Choose a load balancing method. We recommend **Least Connections (Member)**	
	Address	Type the IP Address of the RD Desktop Gateway nodes. This can be an IPv4 or IPv6 address.	
	Service Port	**80** (use **443** if configuring SSL Bridging) Click **Add**, and repeat Address and Port for all nodes	
Profiles (*Main tab-->Local Traffic -->Profiles*)	***TCP*** (*Profiles-->Protocol*)	Name	Type a unique name
		Parent Profile	**tcp-wan-optimized** or **tcp-lan-optimized** depending on where the clients are located
	HTTP (*Profiles-->Services*)	Name	Type a unique name
		Parent Profile	**HTTP**
	Client SSL (*Profiles-->SSL*)	Name	Type a unique name
		Parent Profile	**clientssl**
		Certificate	Select the certificate you imported
		Key	Select the associated key
	Server SSL[2] (*Profiles-->SSL*)	Name	Type a unique name
		Parent Profile	**serverssl**
iRule (*Main tab-->Local Traffic -->iRules*)	*This iRule is used for persistence. It 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.*		
	Name	Type a unique name.	

	Definition	`when HTTP_REQUEST {`
		`  if { [HTTP::header exists "RDG-Connection-Id"] } {`
		`  persist uie [HTTP::header "RDG-Connection-Id"]`
		`  } else {`
		`  persist source_addr`
		`  }`
		`}`	

BIG-IP LTM Object	Non-default settings/Notes	
Virtual Server (*Main tab-->Local Traffic -->Virtual Servers*)	***Name***	Type a unique name.
	Address	Type the IP Address for the virtual server
	Service Port	**443**
	Protocol Profile (client)[1]	Select the TCP profile you created above
	Protocol Profile (server)[1]	Select the TCP profile you created above
	HTTP Profile	Select the HTTP profile you created above
	SSL Profile (Client)	Select the Client SSL profile you created above
	SSL Profile (Server)	*If configuring SSL Bridging Only*: Select the Server SSL profile you created above
	SNAT Pool [3]	**Auto Map** (optional; see footnote [3])
	iRules	Enable the iRule you created above
	Default Pool	Select the pool you created above

[1] You must select **Advanced** from the **Configuration** list for these options to appear
[2] A Server SSL profile is only required if you are configuring SSL Bridging
[3] *If want to use SNAT, and you have a large deployment expecting more than 64,000 simultaneous connections, you must configure a SNAT Pool with an IP address for each 64,000 simultaneous connections you expect. See the BIG-IP documentation on configuring SNAT Pools.*

Supporting RemoteFX for Remote Desktop Gateway (optional)

If you are using Microsoft RemoteFX for Remote Desktop Services, use the following table to configure additional BIG-IP LTM objects for the Remote Desktop Gateway servers.

BIG-IP LTM Object	Non-default settings/Notes		
Health Monitor (*Main tab-->Local Traffic -->Monitors*)	**UDP Monitor**		
	Name	Type a unique name	
	Type	**UDP**	
	Interval	**30** (recommended)	
	Timeout	**91** (recommended)	
	Gateway ICMP Monitor		
	Name	Type a unique name	
	Type	**Gateway ICMP**	
	Interval	**30** (recommended)	
	Timeout	**91** (recommended)	
Pool (*Main tab-->Local Traffic -->Pools*)	***Name***	Type a unique name	
	Health Monitor	Select both monitors you created above (ensure *Availability Requirement* is set to **All** (the default)	
	Slow Ramp Time[1]	**300**	
	Load Balancing Method	Choose a load balancing method. We recommend **Least Connections (Member)**	
	Address	Type the IP Address of a Remote Desktop Gateway device	
	Service Port	**3391** Click **Add**, and repeat Address and Port for all Remote Desktop Gateway devices	
Profiles (*Main tab-->Local Traffic -->Profiles*)	***Persistence*** (*Profiles-->Persistence*)	Name	Type a unique name
		Persistence Type	**Source Address Affinity**
		Match Across Services	**Enabled**

BIG-IP LTM Object	Non-default settings/Notes	
Virtual Servers (*Main tab-->Local Traffic -->Virtual Servers*)	**Remote Desktop Session Host virtual server**	
	Name	Type a unique name.
	Address	Type the same IP Address you used for the Remote Desktop Gateway virtual server on the previous page.
	Service Port	**3391**
	SNAT Pool [2]	**Auto Map** (optional; see footnote [2])
	Default Pool	Select the Remote Desktop Gateway pool you created above
	Default Persistence Profile	Select the Persistence profile you created

[1] *You must select **Advanced** from the **Configuration** list for these options to appear*
[2] *If want to use SNAT, and you have a large deployment expecting more than 64,000 simultaneous connections, you must configure a SNAT Pool with an IP address for each 64,000 simultaneous connections you expect. See the BIG-IP documentation on configuring SNAT Pools.*

Modifying the RD Gateway virtual server to use the Persistence profile you created

The final task is to modify the Remote Desktop Gateway virtual server you configured (using the guidance on the previous page) to use the persistence profile you just created for RemoteFX as a fallback method.

To modify the virtual server

1. Expand **Local Traffic** and then click **Virtual Servers**.
2. Click the name of the TCP RD Gateway virtual server you created using the guidance from the table on page 5.
3. On the Menu bar, click **Resources**.
4. From the **Fallback Persistence Profile** list, select the name of the Source Address Affinity persistence profile you just created.
5. Click **Update**. This completes the RemoteFX configuration.

Deploying a reverse proxy virtual server for Remote Desktop Gateway

This section describes how to publish Remote Desktop Gateway services in a perimeter or DMZ network. This virtual server forwards traffic to the internal virtual server you just created.

Configuration table for the reverse proxy virtual server

BIG-IP LTM Object	Non-default settings/Notes	
Health Monitors (*Main tab-->Local Traffic -->Monitors*)	***Name***	Type a unique name
	Type	**HTTP** (use **HTTPS** if configuring SSL Bridging)
	Interval	**30** (recommended)
	Timeout	**91** (recommended)
	Send String *(one line, and replace red text with your host name)*	**RPC_IN_DATA /rpc/en-us/rpcproxy.dll HTTP/1.1\r\nHost: rdg.example.com**
	Receive String	**200 Success**
	User Name	Type the user name of an account with RDG access.
	Password	Type the associated password

BIG-IP LTM Object	Non-default settings/Notes		
Pool (*Main tab-->Local Traffic -->Pools*)	***Name***	Type a unique name	
	Health Monitor	Select the monitor you created above	
	Address	Only add the IP address for the internal Remote Desktop Gateway virtual server you created	
	Service Port	**443**	
Profiles (*Main tab-->Local Traffic -->Profiles*)	***TCP*** (*Profiles-->Protocol*)	Name	Type a unique name
		Parent Profile	Use **tcp-wan-optimized** or **tcp-lan-optimized** depending on where your clients are located.
	Client SSL (*Profiles-->SSL)*	Name	Type a unique name
		Parent Profile	**clientssl**
		Certificate	Select the certificate you imported
		Key	Select the associated key
	Server SSL[2] (*Profiles-->SSL)*	Name	Type a unique name
		Parent Profile	**serverssl**
Virtual Server (*Main tab-->Local Traffic -->Virtual Servers*)	***Name***	Type a unique name.	
	Address	Type the External IP address for Remote Desktop Gateway connections as the IP address for this virtual server	
	Service Port	**443**	
	Protocol Profile (client)[1]	Select the TCP profile you created above	
	Protocol Profile (server)[1]	Select the TCP profile you created above	
	SSL Profile (Client)	Select the Client SSL profile you created above	
	SSL Profile (Server)	*If configuring SSL Bridging Only*: Select the Server SSL profile you created above	
	SNAT Pool [2]	**Auto Map** (optional; see footnote [2])	
	Default Pool	Select the pool you created above	

[1] You must select **Advanced** from the **Configuration** list for these options to appear

[2] *If want to use SNAT, and you have a large deployment expecting more than 64,000 simultaneous connections, you must configure a SNAT Pool with an IP address for each 64,000 simultaneous connections you expect. See the BIG-IP documentation on configuring SNAT Pools.*

This completes the configuration for this scenario.

Scenario 3: Configuring the BIG-IP LTM for the Remote Desktop Connection Broker service

Use this scenario if you have configured high availability for RD Connection Broker (available in Windows Server 2012 and 2012 R2 only). In this case, BIG-IP LTM load balances requests from the Remote Desktop Gateway servers to the Connection Broker service between all members of the RD Connection Broker farm.

Prerequisites for this scenario

- The following are requirements for the RD Connection Broker farm:
  - RD Connection Broker role is installed.
  - Members should match those in the BIG-IP LTM pool.
  - Remote Desktop Connection Broker is configured in High Availability mode.
  - Farm name must be a DNS name that resolves to the BIG-IP LTM Connection Broker virtual server IP address.

Configuration table for scenario 3

The table on the following page contains a list of BIG-IP LTM configuration objects along with any non-default settings you should configure as a part of this deployment scenario. Unless otherwise specified, settings not mentioned in the table can be configured as applicable for your configuration. For specific instructions on configuring individual objects, see the online help or product manuals.

BIG-IP LTM Object	Non-default settings/Notes	
Health Monitor[1] (*Main tab-->Local Traffic -->Monitors*)	***Name***	Type a unique name
	Type	**TCP**
	Interval	**30** (recommended)
	Timeout	**91** (recommended)
	Send String[1] *(use the string for your version of Windows Server*	**Window Server 2012 R2**
		\x03\x00\x00\x13\x0E\xE0\x00\x00\x00\x00\x00\x01\x00\x08\x00\x0b\x00\x00\x00
		Window Server 2012, 2008 R2
		\x03\x00\x00\x13\x0E\xE0\x00\x00\x00\x00\x00\x01\x00\x08\x00\x03\x00\x00\x00
	Receive String[1] *(use the string for your version of Windows Server)*	**Window Server 2012 R2**
		\x03\x00\x00\x13\x0E\xD0\x00\x00\x12\x34\x00\x02\x0f\x08\x00\x08\x00\x00\x00
		Window Server 2012
		\x03\x00\x00\x13\x0E\xD0\x00\x00\x12\x34\x00\x02\x07\x08\x00\x02\x00\x00\x00
		Window Server 2008 R2[2]
		\x03\x00\x00\x13\x0E\xD0\x00\x00\x12\x34\x00\x02\x09\x08\x00\x02\x00\x00\x00
Pool (*Main tab-->Local Traffic -->Pools*)	***Name***	Type a unique name
	Health Monitor	Select the monitor you created above
	Slow Ramp Time[3]	**300**
	Load Balancing Method	Choose a load balancing method. We recommend **Least Connections (Member)**
	Address	Type the IP Address of the RD Connection Broker nodes. This can be an IPv4 or IPv6 address.
	Service Port	**3389** Click **Add**, and repeat Address and Port for all nodes

[1] If you are using BIG-IP version 11.5.x, see *Troubleshooting on page 23*
[2] If you are using Windows Server 2008 R2, this Receive String was modified in this version of the guide, see *Troubleshooting on page 23*
[3] You must select **Advanced** from the **Configuration** list for these options to appear

BIG-IP LTM Object	Non-default settings/Notes		
Profiles (*Main tab-->Local Traffic -->Profiles*)	***TCP*** (*Profiles-->Protocol*)	Name	Type a unique name
		Parent Profile	Use **tcp-wan-optimized** or **tcp-lan-optimized** depending on where your clients are located.
		Nagle's Algorithm	If you selected *tcp-wan-optimized*: Clear the **Nagle's Algorithm** box to disable Nagle's Algorithm.
	Persistence (*Profiles-->Persistence)*	Name	Type a unique name
		Persistence Type	**Microsoft® Remote Desktop**
		Has Session Directory	Check the **Has Session Directory** box.
Virtual Server (*Main tab-->Local Traffic -->Virtual Servers*)	***Name***	Type a unique name.	
	Address	Type the IP Address for the virtual server. This IP address must match the IP address configured in DNS for the Connection Broker Farm Name.	
	Service Port	**3389**	
	Protocol Profile (client)[1]	Select the TCP profile you created above	
	Protocol Profile (server)[1]	Select the TCP profile you created above	
	SNAT Pool [2]	**Auto Map** (optional; see footnote [3])	
	Default Pool	Select the pool you created above	

[1] You must select **Advanced** from the **Configuration** list for these options to appear

[2] *If want to use SNAT, and you have a large deployment expecting more than 64,000 simultaneous connections, you must configure a SNAT Pool with an IP address for each 64,000 simultaneous connections you expect. See the BIG-IP documentation on configuring SNAT Pools.*

This completes the configuration for this scenario.

Scenario 4: Adding Remote Desktop Web Access to BIG-IP LTM

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 preconfigured 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 than used for the Gateway servers, whether or not the Gateway roles are installed on the same devices.

If you want to use the same IP address for both Remote Desktop Gateway and Remote Desktop Web Access, before starting this section, see *Optional: Using a combined virtual server for Remote Desktop Gateway and Remote Desktop Web Access on page 22.*

Prerequisites and configuration notes

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.

- Install the Remote Desktop Web Access role on at least one server; for load-balancing connections, you will need at least two servers. See this Microsoft document: *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.
- The DNS name that will be used by the BIG-IP 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 6).
- For Remote Desktop Web Access, you must either configure the BIG-IP system for SSL Bridging or no encryption as shown in the configuration table.

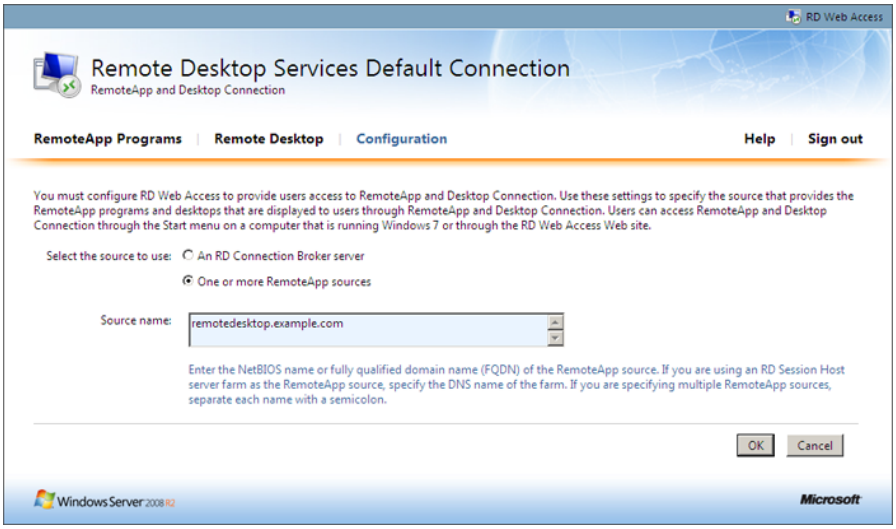

Figure 6: *Remote Desktop Services default connection page (2008 R2)*

Configuration table

The following table contains a list of BIG-IP LTM configuration objects along with any non-default settings you should configure as a part of this deployment scenario. Unless otherwise specified, settings not mentioned in the table can be configured as applicable for your configuration. For specific instructions on configuring individual objects, see the online help or product manuals.

BIG-IP LTM Object	Non-default settings/Notes		
Health Monitor (*Main tab-->Local Traffic -->Monitors*)	***Name***	Type a unique name	
	Type	**HTTP** (use **HTTPS** if configuring SSL Bridging)	
	Interval	**30** (recommended)	
	Timeout	**91** (recommended)	
	Send String	**GET /RDWeb/Pages/en-US/login.aspx HTTP/1.1\r\nHost: rdwa.example.com\r\nConnection: Close\r\n\r\n** *(replace red text with your host name)*	
	Receive String	**200 OK**	
	User Name	Type a valid user name in your Active Directory domain	
	Password	Type the associated password	
Pool (*Main tab-->Local Traffic -->Pools*)	***Name***	Type a unique name	
	Health Monitor	Select the monitor you created above	
	Slow Ramp Time[1]	**300**	
	Load Balancing Method	Choose a load balancing method. We recommend **Least Connections (Member)**	
	Address	Type the IP Address of the RD Web Access nodes. This can be an IPv4 or IPv6 address.	
	Service Port	**80** (use **443** if configuring SSL Bridging) Click **Add**, and repeat Address and Port for all nodes	
Profiles (*Main tab-->Local Traffic -->Profiles*)	***TCP*** (*Profiles-->Protocol*)	Name	Type a unique name
		Parent Profile	Use **tcp-wan-optimized** or **tcp-lan-optimized** depending on client locatation.
	Persistence (*Profiles-->Persistence*)	Name	Type a unique name
		Persistence Type	**Cookie**
	HTTP (*Profiles-->Services*)	Name	Type a unique name
		Parent Profile	**http**
		Redirect Rewrite[2]	**All**[2]
	Client SSL (*Profiles-->SSL*)	Name	Type a unique name
		Parent Profile	**clientssl**
		Certificate and Key	Select the certificate and key you imported
	Server SSL[2] (*Profiles-->SSL*)	Name	Type a unique name
		Parent Profile	**serverssl**
Virtual Servers (*Main tab-->Local Traffic -->Virtual Servers*)	**Remote Desktop Web Access main virtual server**		
	Name	Type a unique name.	
	Address	Type the IP Address for the virtual server	
	Service Port	**443**	
	Protocol Profile (client)[1]	Select the TCP profile you created above	
	Protocol Profile (server)[1]	Select the TCP profile you created above	
	HTTP Profile	Select the HTTP profile you created above	
	SSL Profile (Client)	Select the Client SSL profile you created above	
	SSL Profile (Server)	*If configuring SSL Bridging Only*: Select the Server SSL profile you created above	
	SNAT Pool [3]	**Auto Map** (optional; see footnote [3])	
	Default Pool	Select the pool you created above	
	Persistence Profile	Select the Persistence profile you created	

[1] *You must select **Advanced** from the **Configuration** list for these options to appear*
[2] *Only necessary if offloading SSL*
[3] *If want to use SNAT, and you have a large deployment expecting more than 64,000 simultaneous connections, you must configure a SNAT Pool with an IP address for each 64,000 simultaneous connections you expect. See the BIG-IP documentation on configuring SNAT Pools.*

BIG-IP LTM Object	Non-default settings/Notes	
Virtual Servers (cont) (*Main tab-->Local Traffic -->Virtual Servers*)	**Port 135 virtual server**	
	Name	Type a unique name.
	Address	Type the IP Address for the virtual server
	Service Port	**135**
	SNAT Pool [3]	**Auto Map** (optional; see footnote [3])
	Default Pool	Select the pool you created above
	Persistence Profile	**source_addr**

This completes the configuration for scenario 4.

Scenario 5: Publishing Remote Desktop Resources using BIG-IP APM

F5's Access Policy Manager allows you to securely publish Remote Desktop connections and programs, which users can access using links on an APM Webtop. This can eliminate the need to locate a Remote Desktop Web Access server in the DMZ or perimeter network. This section shows how to publish both a Remote Desktop connection and an individual program using APM.

Prerequisites and configuration notes

The following are prerequisites and notes specific to this scenario.

- You must have BIG-IP APM or Edge Gateway licensed and provisioned on your BIG-IP system. For more information, contact your F5 sales representative.
- The BIG-IP system running APM must have a route to the Remote Desktop servers. For information on creating Routes on the BIG-IP system, see the BIG-IP documentation.
- You must have DNS and NTP configured on the BIG-IP system. See *Appendix C: Configuring DNS and NTP settings on the BIG-IP system on page 28.*
- You must have imported a valid SSL certificate and key for use in the Client SSL profile.
- BIG-IP APM does not yet support connections to Remote Desktop resources from Windows 8. We will update this guide when Windows 8 is supported.
- If you are publishing programs to an APM Webtop, you must have either:
  - Configured each program as a **RemoteApp** program in Remote Desktop Services,
  - Modified the following Windows Group Policy setting:
    Computer Configuration>Administrative Templates>Windows Components>Remote Desktop Services>Remote Desktop Session Host>Connections>Allow remote start of unlisted programs>Enabled

Configuring the BIG-IP APM

Use the following table to create the BIG-IP Edge Gateway or APM configuration. Create the objects in the order they appear in the table. For specific instructions on configuring individual objects, see the product documentation.

BIG-IP Object	Non-default settings/Notes	
Remote Desktop (*Access Policy--> Application Access--> Remote Desktops*))	***Name***	Type a unique name.
	Type	**RDP**
	Destination	Type the host name of the RDP server. Alternatively, click the IP Address button and then type the IP address
	Port	**3389**
	Auto Logon	Check the box to enable Auto Logon
	Caption	If necessary, type the appropriate caption. By default, the Caption is the value for Name you typed above.
	Optional: Use the following settings to restrict access to a specific application instead of a full RDP logon	
	Application to Start	Type the name of the application (i.e. calc.exe or notepad.exe)
	Working Directory	Type the directory where the application resides (i.e. C:\Windows\System32 for Calculator or Notepad)
AAA Server (*Access Policy-->AAA Servers*)	***Name***	Type a unique name.
	Type	**Active Directory**
	Domain Controller	Type the IP address or FQDN name of an Active Directory Domain Controller
	Domain Name	Type the Active Directory domain name
	Admin Name[1]	Type the AD user name with administrative permissions (optional)
	Admin Password[1]	Type the associated password (optional). Verify the Password

[1] Optional. Admin Name and Password are required if anonymous binding to Active Directory is not allowed.

BIG-IP Object	Non-default settings/Notes	
Connectivity Profile (*Access Policy-->Secure Connectivity*)	***Name***	Type a unique name. All other fields are optional.
Webtop (*Access Policy-->Webtops*)	***Name***	Type a unique name.
	Type	**Full**
Access Profile *(Access Policy-->Access Profiles)*	***Name***	Type a unique name.
	Language	Select the appropriate language and move it to the **Accepted Languages** box.
Access Policy	***Edit***	Edit the Access Profile using the Visual Policy Editor using the following procedure.

Configuring the Access Policy

After creating the objects in the table above, use the following procedure to edit the Access Policy on the BIG-IP APM using the Visual Policy Editor (VPE).

To configure the Access Policy

1. On the Main tab, expand **Access Policy**, and click **Access Profiles**.
2. Locate the Access Profile you created using the table above, and then, in the Access Policy column, click **Edit**. The VPE opens in a new window.
3. Click the **+** symbol between **Start** and **Deny**. A box opens with options for different actions.
4. Click the **Logon Page** option button, and then the **Add Item** button at the bottom.
5. In row #3, perform the following:
   a. From the **Type** list, select **text** from the list.
   b. In the **Post Variable Name** box, type **domain**.
   c. In the **Session Variable Name** box, type **domain**.
   d. In the Customization section, in the Logon Page Input Field #3 box, type **Domain**.
   e. Configure any other settings as applicable, and then click **Save**. In our example, we leave the defaults.
6. Click the **+** symbol between **Logon Page** and **Deny**. A box opens with options for different actions.
7. Click the **AD Auth** option button, and then click **Add Item**.
   a. From the Server list, select the AAA Server you created using the table on the previous page.
   b. Click **Save**.
8. On the *Successful* path, click the **+** symbol between **AD Auth** and **Deny**. A box opens with options for different actions.
9. Click the **Advanced Resource Assign** option button (v11.4 and later) or **Full Resource Assign** (v11.3), and then click **Add Item**.
   a. Click the **Add New entry** button.
   b. In the Expression box that appears, click **Add/Delete**.
   c. Click the Remote Desktop tab, and then check the box for the Remote Desktop object you created.
   d. Click the Webtop tab, and then click the button for the Webtop object you created.
   e. Click **Update**.
   f. Click **Save**.
10. Click the **Deny** box on the path leading from Advanced (or Full) Resource Assign.

11. Click the **Allow** option button, and then click **Save**.
12. Click the yellow **Apply Access Policy** link in the upper left part of the window. You must apply an Access Policy before it takes effect.

Creating the profiles

For this configuration, you must create a Client SSL profile and a HTTP profile. Use the following table:

BIG-IP Object	Non-default settings/Notes	
HTTP (*Local Traffic-->Profiles-->Services*)	Name	Type a unique name
	Parent Profile	**http**
Client SSL (*Local Traffic-->Profiles-->SSL)*	Name	Type a unique name
	Parent Profile	**clientssl**
	Certificate	Select the SSL certificate you imported
	Key	Select the associated key

Configuring the virtual server

The next task is to create a virtual server on the BIG-IP system. Use the following table to configure the virtual server.

BIG-IP Object	Non-default settings/Notes	
Virtual Server (*Main tab-->Local Traffic -->Virtual Servers*)	***Name***	Type a unique name.
	Address	Type the IP Address for the virtual server
	Service Port	**443**
	HTTP Profile	Select the HTTP profile you created above
	SSL Profile (Client)	Select the Client SSL profile you created
	Access Profile	Select the Access profile you created above
	Connectivity Profile	Select the Connectivity profile you created above

This completes the configuration.

Optional: Using a combined virtual server for Remote Desktop Gateway and Remote Desktop Web Access

Depending on your network topology, you may want to use the same IP address for both Remote Desktop Gateway and Remote Desktop Web Access connections. This is optional, and only necessary if you want to use the same IP address for both connection types.

Note

If you are using different FQDNs for Remote Desktop Gateway and Remote Desktop Web Access, both FQDNs must be present in the certificate configured in the client SSL profile attached to the Remote Desktop virtual server.

1. Use the guidance in *Scenario 2: Configuring the BIG-IP LTM for Remote Desktop Access with RD Gateway on page 8* to configure BIG-IP system for Remote Desktop Gateway
2. Use the guidance in *Scenario 4: Adding Remote Desktop Web Access to BIG-IP LTM on page 16,* for creating the Health Monitor and Pool only; do **NOT** create the BIG-IP profiles or virtual server for Remote Desktop Web Access.
3. Create an iRule (**Local Traffic > iRules > Create**), using the following code for the Definition. Replace **my_rdwa_pool** with the name of the BIG-IP pool that contains the Remote Desktop Web Access servers.

```
when HTTP_REQUEST {
    switch -glob -- [string tolower [HTTP::path]] {
        "/rdweb*" -
        "/favicon.ico*" {
            pool my_rdwa_pool
        }
    }
}
```

4. Return to the BIG-IP virtual server you created for Remote Desktop Gateway (**Local Traffic > Virtual Servers >** *name of the TCP RD Gateway virtual server*). Click the Resources tab and then add the iRule you just created.
Important: *Make sure you add the iRule to the TCP virtual server and not the UDP virtual server.*
5. Click Update.

Troubleshooting

Use this section for common troubleshooting tips.

Q: After rebooting the BIG-IP system (or running the command **load sys config**) running version 11.5.x, all pool members are being marked down by the BIG-IP device, even though they are available.

A: This is a known issue in BIG-IP version 11.5.x. After a reboot or loading the system configuration from the command line, the backslashes in the TCP health monitors for the Session Host and Connection Broker scenarios no longer appear. This causes the system to improperly mark the pool members as unavailable. This is not an issue in earlier (or later) versions of the BIG-IP system.

To work around this issue, you must manually reconfigure the Send and Receive Strings for the TCP health monitors using the strings in the configuration table. Alternatively you could upgrade to BIG-IP version 11.6 or later.

Q: Why are the monitors marking Windows 2008 R2 RDSH pool members down after installing Windows Update KB3003743?

A: If you have recently installed Windows update KB3003743 on a Windows 2008 R2 server, the TCP monitor in the manual configuration table in the previous version of this guide would result in pool members being marked down incorrectly. This issue only affects Windows 2008 R2.

To work around this issue, you must update the Receive String in the health monitor. Click **Local Traffic > Monitors> <name of the TCP monitor>**. Use the new Receive String as shown above, and then click **Update**.

Old Receive String: **\x03\x00\x00\x13\x0E\xD0\x00\x00\x12\x34\x00\x02\x01\x08\x00\x02\x00\x00\x00**

New Receive String: **\x03\x00\x00\x13\x0E\xD0\x00\x00\x12\x34\x00\x02\x09\x08\x00\x02\x00\x00\x00**

Appendix A: Configuring WMI monitoring of the RDS servers

If you find your RDS servers are under high performance load, you can dynamically load balance between them using F5's WMI monitor. This monitor checks the CPU, memory, and disk usage of the nodes and, in conjunction with Dynamic Ratio load balancing mode, sends the connection to the server most capable of processing it.

For an overview of the WMI performance monitor, see *http://support.f5.com/kb/en-us/solutions/public/6000/900/sol6914.html*.

Installing the F5 WMI handler

The first task is to copy the F5 WMI handler to the RDS server and configure IIS to use the F5 Data Gathering Agent. For instruction on installing the Data Gathering Agent, see: *http://support.f5.com/kb/en-us/products/big-ip_ltm/manuals/product/ltm_configuration_guide_10_0_0/ltm_appendixb_monitor_considerations.html#1185026*

Be sure to follow the procedures for the version of IIS you are using.

If you want to use the WMI monitor for the Session Host or Connection Broker servers, you must have IIS installed on those devices in order to install the handler.

Creating the WMI Monitor on the BIG-IP LTM

The next task is to create the WMI monitor on the applicable BIG-IP LTM systems. Use the following table:

BIG-IP LTM Object	Non-default settings/Notes	
Health Monitors (*Main tab-->Local Traffic -->Monitors*)	***Name***	Type a unique name
	Type	**WMI**
	Interval	**30** (recommended)
	Timeout	**91** (recommended)
	User Name	Type the appropriate user name
	Password	Type the associated password
	URL:	**/scripts/F5Isapi.dll** (for IIS 6, 7, and 7.5)

Create this monitor on all applicable BIG-IP LTM systems.

Apply the monitor on the BIG-IP LTM devices

Next, we apply the monitor to the applicable RDS nodes on the BIG-IP LTM system. This can be any or all of the BIG-IP LTM devices that are sending traffic to the RDS servers.

To apply the monitor to the nodes

1. On the Main tab, expand **Local Traffic** and then click **Nodes**.
2. From the list of nodes, click a node for the external IP address of your RDS server.
3. In the Configuration section, from the **Health Monitor** list, select **Node Specific**.
4. From the Available list, select the WMI monitor you created, and then click Add (<<).
5. Click **Update**.
6. Repeat for all appropriate nodes.
7. Repeat this procedure for all applicable BIG-IP LTM systems.

Modifying the pool(s) to use the Dynamic Ratio load balancing method

The next task is to modify the BIG-IP LTM pools to use the Dynamic Ratio load balancing method. Make this change for each pool that contains the RDS nodes to which you added the WMI monitor.

To modify the load balancing method on the pool

1. On the Main tab, expand **Local Traffic** and then click **Pools**.
2. Click the name of the appropriate Pool. The Pool Properties page opens.
3. On the Menu bar, click **Members**.
4. From the **Load Balancing Method** list, select **Dynamic Ratio (Node)**.
5. Click the **Update** button.
6. Repeat this procedure for all applicable pools on this BIG-IP LTM.
7. Repeat this procedure on all applicable BIG-IP LTM systems.

Appendix B: Using X-Forwarded-For to log the client IP address in IIS 7.0, 7.5, and 8 (optional)

When you configure BIG-IP LTM to use SNAT, the BIG-IP system replaces the source IP address of an incoming connection with its local self IP address (in the case of SNAT Auto Map), or an address you have configured in a SNAT pool. As a result, Microsoft IIS logs each connection with its assigned SNAT address, rather than the address of the client.

Beginning with IIS 7, Microsoft provides an optional Advanced Logging Feature for IIS that allows you to define custom log definitions that can capture additional information such as the client IP address included in the X-Forwarded-For header.

This section is only applicable if you are deploying Remote Desktop Gateway or Remote Desktop Web Access.

Modifying the HTTP profile to enable X-Forwarded-For

The first task is to modify the HTTP profile created by the template to enable the X-Forwarded-For header.

To modify the HTTP profile

1. On the Main tab, expand **Local Traffic**, and then click **Profiles**.
2. From the HTTP profile list, select the HTTP profile you created.
3. In the Settings section, on the **Insert X-Forwarded-For** row, click the **Custom** box. From the list, select **Enabled**.
4. Click the **Update** button.

Deploying the Custom Logging role service

The first task is to deploy the Custom Logging role service. If you do not deploy this role service, you may receive a "Feature not supported" error when trying to edit the log definition in the next section. If you receive this error, ensure that you are editing the log definition at the server level in IIS Manager.

The configuration is slightly different depending on which version of IIS you are running. Use the procedure applicable to your version of IIS.

To deploy the Custom Logging role service for IIS 7.0 and 7.5 (Windows Server 2008)

1. From your Windows Server 2008 or Windows Server 2008 R2 device, open Server Manager.
2. In the Navigation pane, expand **Roles**.
3. Right-click **Web Server**, and then click **Add Role Services**.
4. Under Health and Diagnostics, check the box for **Custom Logging**, and then click **Next**.
5. On the Confirmation page, click **Install**.
6. After the service has successfully installed, click the **Close** button.

To deploy the Custom Logging role service for IIS 8.0 (Windows Server 2012)

1. From your Windows Server 2012 device, open Server Manager.
2. Click **Manage** and then **Add Roles and Features**.
3. Select Role-based or feature-based installation.
4. On the Roles screen, expand **Web Server (IIS)** and **Health and Diagnostics** and then check the box for **Custom Logging**.
5. Click **Next** and then on the Features screen, click **Next** again.
6. Click **Install**.
7. After the service has successfully installed, click the **Close** button.

Adding the X-Forwarded-For log field to IIS

Before beginning the following procedure, you must have installed IIS Advanced Logging. For installation instructions, see *http://www.iis.net/community/files/media/advancedlogging_readme.htm*

If you are using IIS version 6, F5 has a downloadable ISAPI filter that performs a similar function to the Advanced Logging Feature discussed here. For information on that solution, see the DevCentral post at *http://devcentral.f5.com/weblogs/Joe/archive/2009/08/19/x_forwarded_for_log_filter_for_windows_servers.aspx*

The following procedure is the same for IIS versions 7.0, 7.5, and 8.0.

To add the X-Forwarded-For log field to IIS

1. From your Windows Server device, open the Internet Information Services (IIS) Manager.
2. From the Connections navigation pane, click the appropriate server on which you are configuring Advanced Logging. The Home page appears in the main panel.
3. From the Home page, under IIS, double-click **Advanced Logging**.
4. From the Actions pane on the right, click **Edit Logging Fields**.
5. From the Edit Logging Fields dialog box, click the **Add Field** button, and then complete the following:
    a. In the **Field ID** box, type **X-Forwarded-For**.
    b. From the **Category** list, select **Default**.
    c. From the **Source Type** list, select **Request Header**.
    d. In the **Source Name** box, type **X-Forwarded-For**.
    e. Click the **OK** button.
6. Click a Log Definition to select it. By default, there is only one: %COMPUTERNAME%-Server. The log definition you select must have a status of Enabled.
7. From the Actions pane on the right, click **Edit Log Definition**.
8. Click **Select Fields**, and then check the box for the X-Forwarded-For logging field.
9. Click the **OK** button.
10. From the Actions pane, click **Apply**.
11. Click **Return To Advanced Logging**.
12. In the Actions pane, click **Enable Advanced Logging**.

    Now, when you look at the Advanced Logging logs, the client IP address is included.

Appendix C: Configuring DNS and NTP settings on the BIG-IP system

If you are using BIG-IP APM, before beginning the iApp, you must configure DNS and NTP settings on the BIG-IP system.

Configuring the DNS settings

In this section, you configure the DNS settings on the BIG-IP to point to the appropriate DNS servers.

➲ **Note**: *DNS lookups go out over one of the interfaces configured on the BIG-IP system, not the management interface. The management interface has its own, separate DNS settings.*

➲ **Important:** *The BIG-IP system must have a Route to the DNS server. The Route configuration is found on the Main tab by expanding **Network** and then clicking **Routes**. For specific instructions on configuring a Route on the BIG-IP system, see the online help or the product documentation.*

To configure DNS settings

1. On the Main tab, expand **System**, and then click **Configuration**.
2. On the Menu bar, from the **Device** menu, click **DNS**.
3. In the **DNS Lookup Server List** row, complete the following:
   a. In the **Address** box, type the IP address of the DNS server.
   b. Click the **Add** button.
4. Click **Update**.

Configuring the NTP settings

The next task is to configure the NTP settings on the BIG-IP system for authentication to work properly. You must also configure NTP if configuring the BIG-IP GTM as shown in the optional configuration sections.

To configure NTP settings

1. On the Main tab, expand **System**, and then click **Configuration**.
2. On the Menu bar, from the **Device** menu, click **NTP**.
3. In the **Address** box, type the fully-qualified domain name (or the IP address) of the time server that you want to add to the Address List.
4. Click the **Add** button.
5. Click **Update**.

To verify the NTP setting configuration, you can use the **ntpq** utility. From the BIG-IP command line, run **`ntpq -np`**.

See *http://support.f5.com/kb/en-us/solutions/public/10000/200/sol10240.html* for more information on this command.

Document Revision History

Version	Description	Date
1.0	New Version	N/A
2.0	Updated for Windows Server 2012 Remote Desktop Services. Added optional WMI monitor configuration in Appendix A.	08-06-2012
2.1	Modified the port for the Session Host virtual server on page 6 from 443, to the correct port: 3389.	09-04-2012
2.2	Added guidance in the table for scenario 1 to disable Nagle's Algorithm if using the tcp-wan-optimized TCP profile.	09-26-2012
2.3	Updated the guide to include *Scenario 5: Publishing Remote Desktop Resources using BIG-IP APM on page 19.*	10-10-2012
2.4	Removed an unnecessary row for adding a persistence profile to the virtual server in the *Configuration table for scenario 2 on page 10*	04-11-2013
2.5	- Added optional configuration sections for supporting RemoteFX for RD Session Hosts and RD Gateway - Added a virtual server on port 135 to the Remote Desktop Web Access configuration table - Added support for BIG-IP versions 11.3 and 11.4.	08-16-2013
2.6	- Added support for Windows Server 2012 R2 Remote Desktop Services - Added support for BIG-IP version 11.4.1 - Added new Windows Server 2012 R2 RD Services Send and Receive Strings for the monitor for scenario 1	11-01-2013
2.7	Moved the BIG-IP configuration for RDS deployments that have configured high availability for the RD Connection Broker Service out of Scenario 1 and into a new *Scenario 3: Configuring the BIG-IP LTM for the Remote Desktop Connection Broker service on page 14*.	02-13-2014
2.8	- Added a Webtop object to the APM configuration table in *Scenario 5: Publishing Remote Desktop Resources using BIG-IP APM on page 19.* Updated the Access Policy configuration to include selecting both the Webtop and Remote Desktop objects. - Added an additional prerequisite to the same section. - Added support for BIG-IP v11.5 and v11.5.1	03-27-2014
2.9	Corrected the health monitors in *Configuration table for scenario 2 on page 10*. The two monitor scenario was erroneously attributed to Windows Server 2012.	05-06-2014
3.0	- Clarified that the guidance on page 5 for the members should not participate in Connection Broker load balancing as specific to Windows Server 2008 R2. - In the prerequisites for scenario 3 on page 15, removed two prerequisites: “Members should not participate in Connection Broker load balancing” and “Members should use token redirection." This is because Connection Broker HA is only available in Windows 2012 and 2012 R2 and it implies token redirection.	06-25-2014
3.1	Added the new section *Troubleshooting on page 23* with an entry regarding the health monitors if using BIG-IP v11.5.x.	07-31-2014
3.2	Added support for BIG-IP version 11.6	08-25-2014
3.3	- Removed multiple monitor options for different versions of Windows Server from *Scenario 2: Configuring the BIG-IP LTM for Remote Desktop Access with RD Gateway on page 8.* There is now only one monitor for this scenario. - Added a note in the prerequisites and scenario 1 about the new iApp template available on DevCentral for Remote Desktop Session Host (https://devcentral.f5.com/wiki/iApp.Microsoft-Remote-Desktop-Session-Host-iApp.ashx).	09-08-2014
3.4	Added the new section *Optional: Using a combined virtual server for Remote Desktop Gateway and Remote Desktop Web Access on page 22* with guidance on using the same virtual server for these two services.	11-14-2014
3.5	Added a note on page 1 referring to the new iApp templates for Remote Desktop Gateway and Remote Desktop Session Host available on downloads.f5.com, and the associated deployment guide on f5.com.	12-16-2014
3.6	- Modified the health monitor Receive String for Windows Server 2008 R2 due to a Windows Update. - Added a new Troubleshooting entry on *page 23* with instructions on modifying the health monitor Receive String for both manual and iApp configurations.	01-02-2015
3.7	Added a note this guide has been archived, which includes links to the newer guides for Remote Desktop Services.	06-10-2015

F5 Networks, Inc. 401 Elliott Avenue West, Seattle, WA 98119 888-882-4447 www.f5.com

F5 Networks, Inc.
Corporate Headquarters
info@f5.com

F5 Networks
Asia-Pacific
apacinfo@f5.com

F5 Networks Ltd.
Europe/Middle-East/Africa
emeainfo@f5.com

F5 Networks
Japan K.K.
f5j-info@f5.com