Progress®
Kemp® LoadMaster®

Deployment Guide Remote Desktop Services

Generated on: 16 September 2024

Copyright

Visit the following page online to see Progress Software Corporation's current Product Documentation Copyright Notice/Trademark Legend: Product Documentation Copyright Notice & Trademarks | Progress

Table of Contents

Chapter 1: Introduction 4

Document Purpose 4

Intended Audience 5

Chapter 2: RDS Load Balancing Scenarios 6

Scenarios Explained 7

Load Balancing Remote Desktop Web Access 7

Load Balancing Remote Desktop Gateway 8

Load Balancing Remote Desktop Connection Broker 10

Load Balancing Remote Desktop Session Host 12

Deploying the Scenarios 15

Template 15

Prerequisites 15

Implementing Remote Desktop Web Access Load Balancing 16

Implementing Remote Desktop Gateway Load Balancing 22

Implementing Remote Desktop Connection Broker Load Balancing 35

Implementing Remote Desktop Session Host Load Balancing 41

Chapter 3: Troubleshooting 47

Chapter 4: References 49

1

Introduction

Remote Desktop Services (RDS), known as Terminal Services in Windows Server 2008 and earlier, is one of the components of Microsoft Windows that allows a user to take control of a remote computer or virtual machine over a network connection. RDS is Microsoft's implementation of thin client, where Windows software and the entire desktop of the computer running RDS are made accessible to a remote client machine that supports Remote Desktop Protocol (RDP).

With Windows Server 2012 and Windows 8, Microsoft introduced RDP 8.0. The protocol evolved in RDP 8.1 with Windows Server 2012 R2 and Windows 8.1. Compared to previous releases, there have been several changes to both the administrative experience and user experience.

Related Links

For details, see the following topics:

- Document Purpose
- Intended Audience

Document Purpose

This deployment guide provides instructions on how to configure the LoadMaster to load balance the various Microsoft RDS roles in Windows Server 2012 R2.

The Scenarios Explained section discusses the various scenarios in which the LoadMaster can be used. The Deploying the Scenarios section explains the process of setting up load balancing for those scenarios. The References section contains a summary of useful resources regarding RDS (and load balancing RDS) in

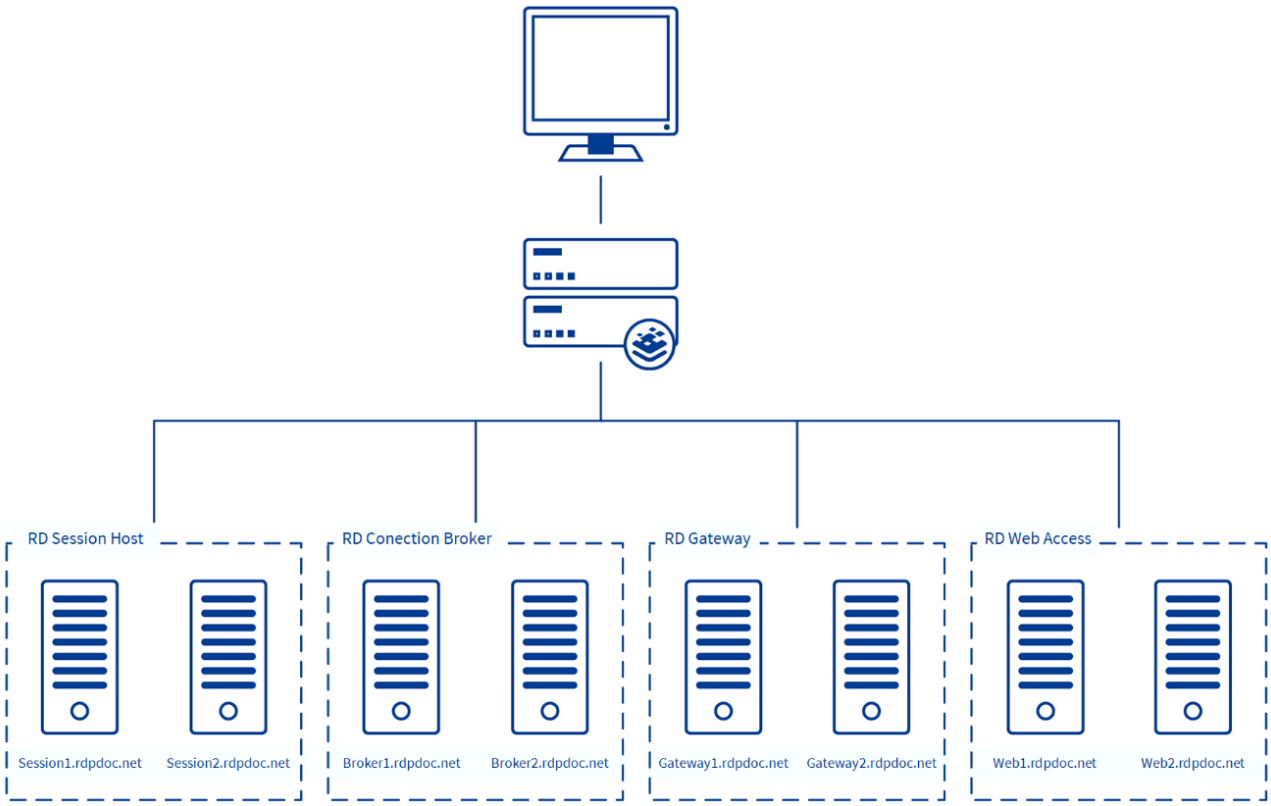
general.

Intended Audience

Anyone interested in configuring the LoadMaster to load balance RDS.

2

RDS Load Balancing Scenarios



The figure above shows the various scenarios where the LoadMaster can be used to load balance RDS

services.

Related Links

For details, see the following topics:

- Scenarios Explained
- Deploying the Scenarios

Scenarios Explained

RDS running on Windows Server 2012 (R2) consists of various different RDS roles. The LoadMaster can be configured to load balance those roles. The sections below discuss the various scenarios in which the LoadMaster can be used to load balance RDS to.

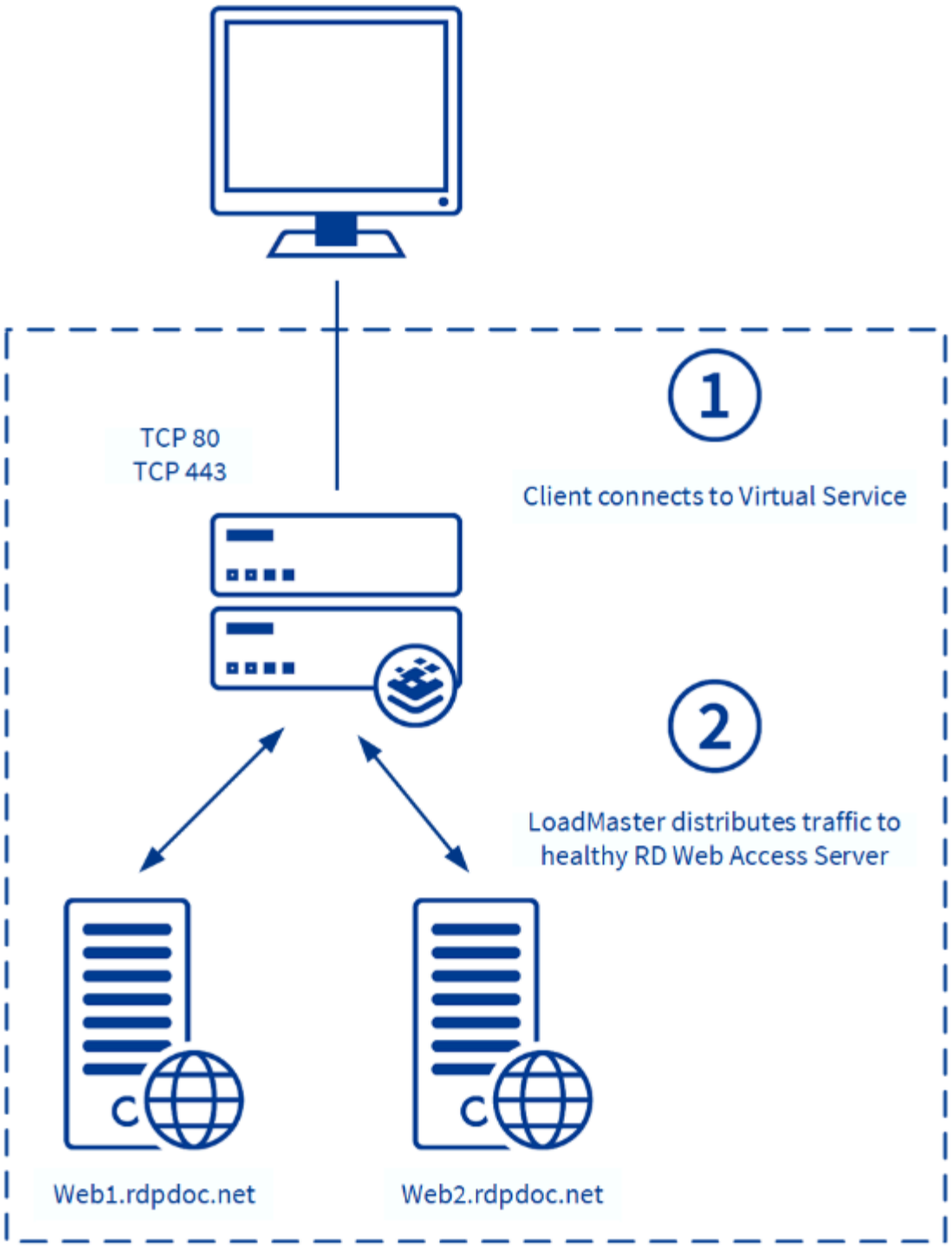
Load Balancing Remote Desktop Web Access

Microsoft Remote Desktop Web Access (RD Web Access) is used to publish Full Desktops as well as Remote Apps and make them available from a website and a web feed.

RD Web Access is a website running on Internet Information Server (IIS). RD Web Access preferably runs on port 443 to leverage SSL security and is, by default, accessed by browsing to **https://<FullyQualifiedDomainName(FQDN)>/rdweb**.



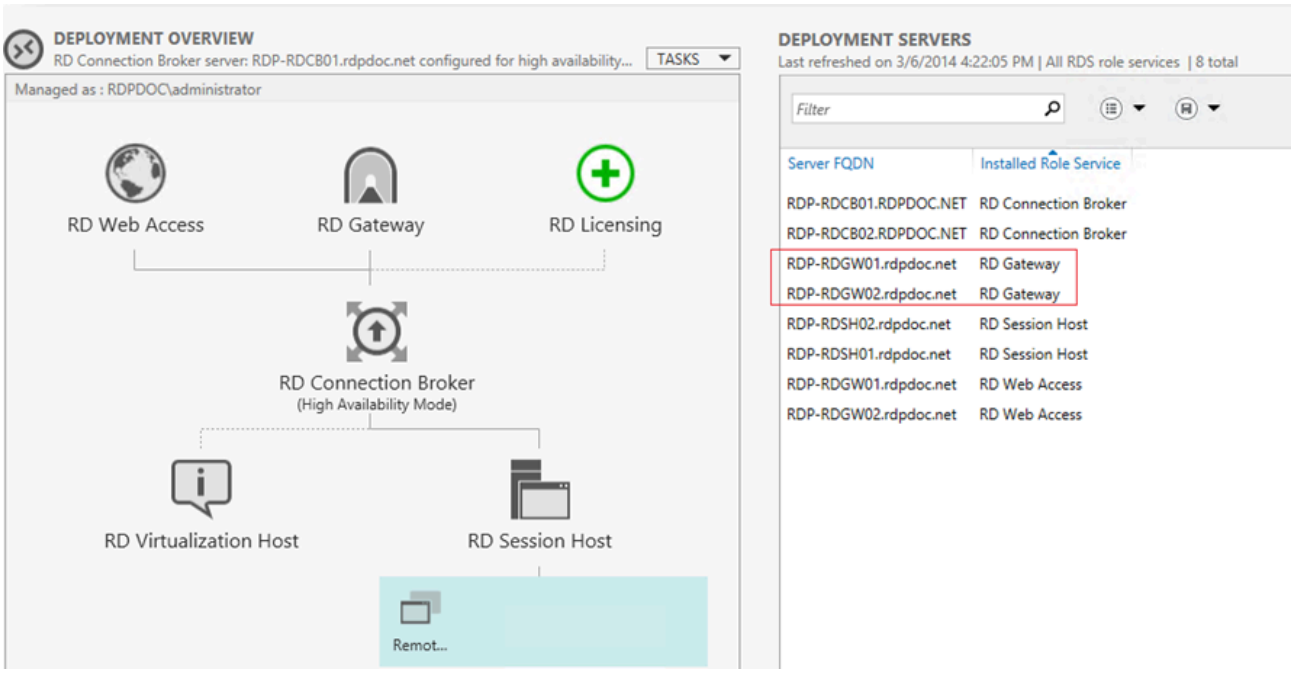
After your RD Web Access server has been installed, you can use the Remote Desktop Management Services (RDMS) console as part of the Server Manager to retrieve the URLs of the RD Web Access servers that are part of the deployment. These servers must be added to the LoadMaster to start load balancing Web Access.



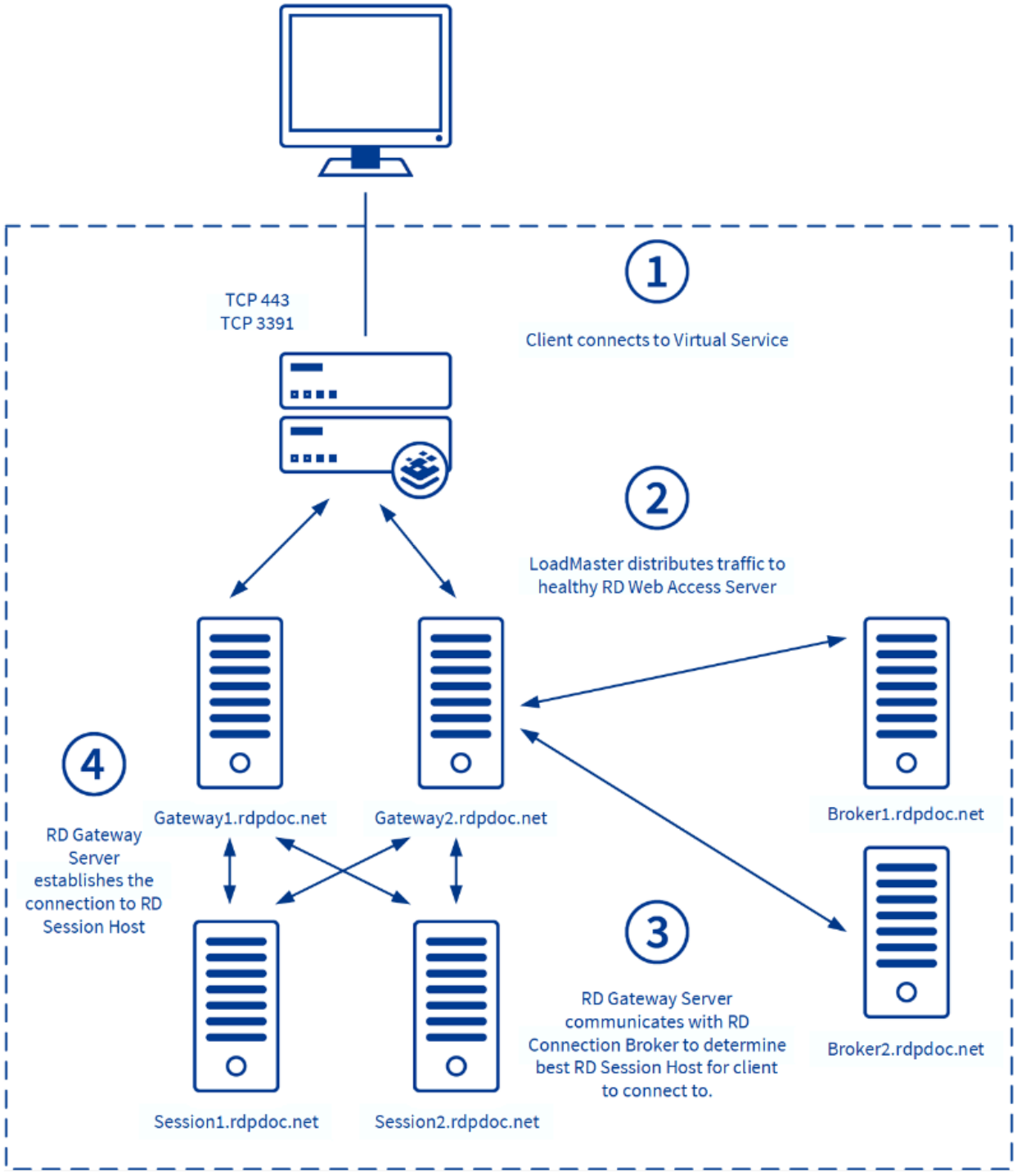
Load Balancing Remote Desktop Gateway

Microsoft Remote Desktop Gateway (RD Gateway) is used to safely publish a Remote App of Full Desktop over the internet. The RD Gateway functions as an RDP proxy. It proxies incoming RDP traffic (on port 443) to the Remote Desktop Session Host (RD Session Host) servers on port 3389.

The RDP traffic running on port 443 must be load balanced in the LoadMaster.



After the RD Gateway role is installed, you can use the Remote Desktop Management Services (RDMS) console as part of the Server Manager to retrieve the RD Gateway servers as part of the deployment.

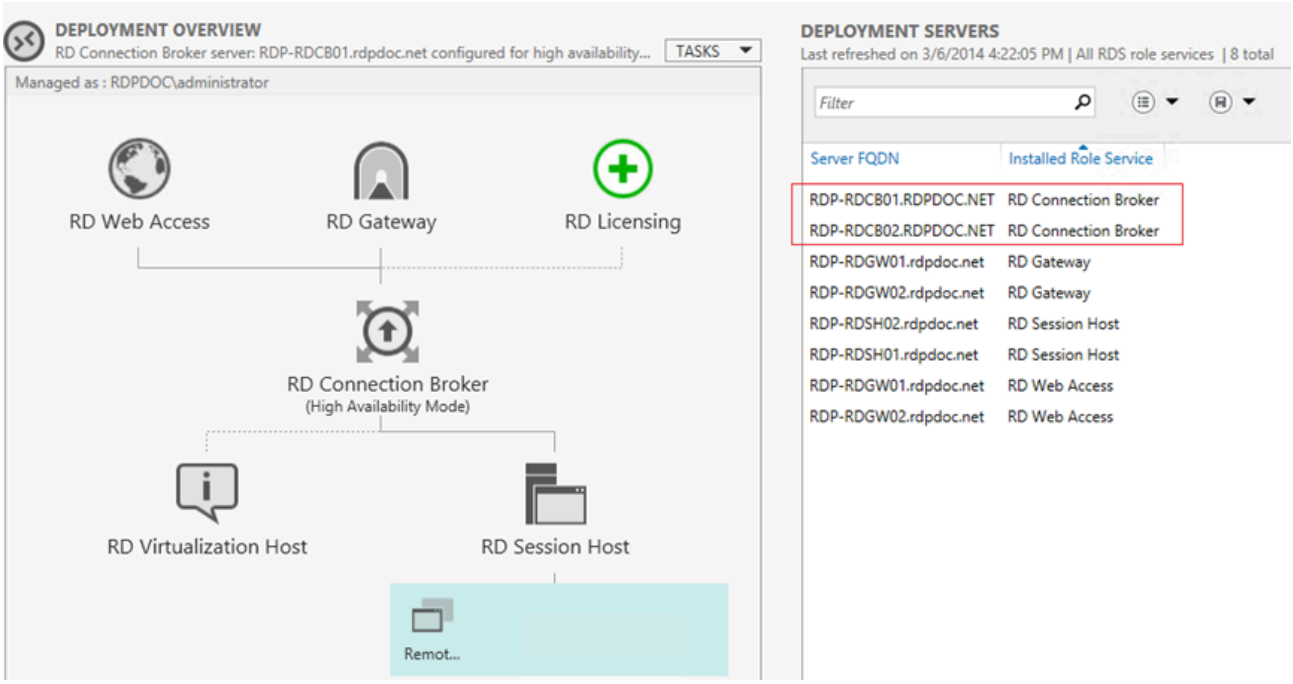


Load Balancing Remote Desktop Connection Broker

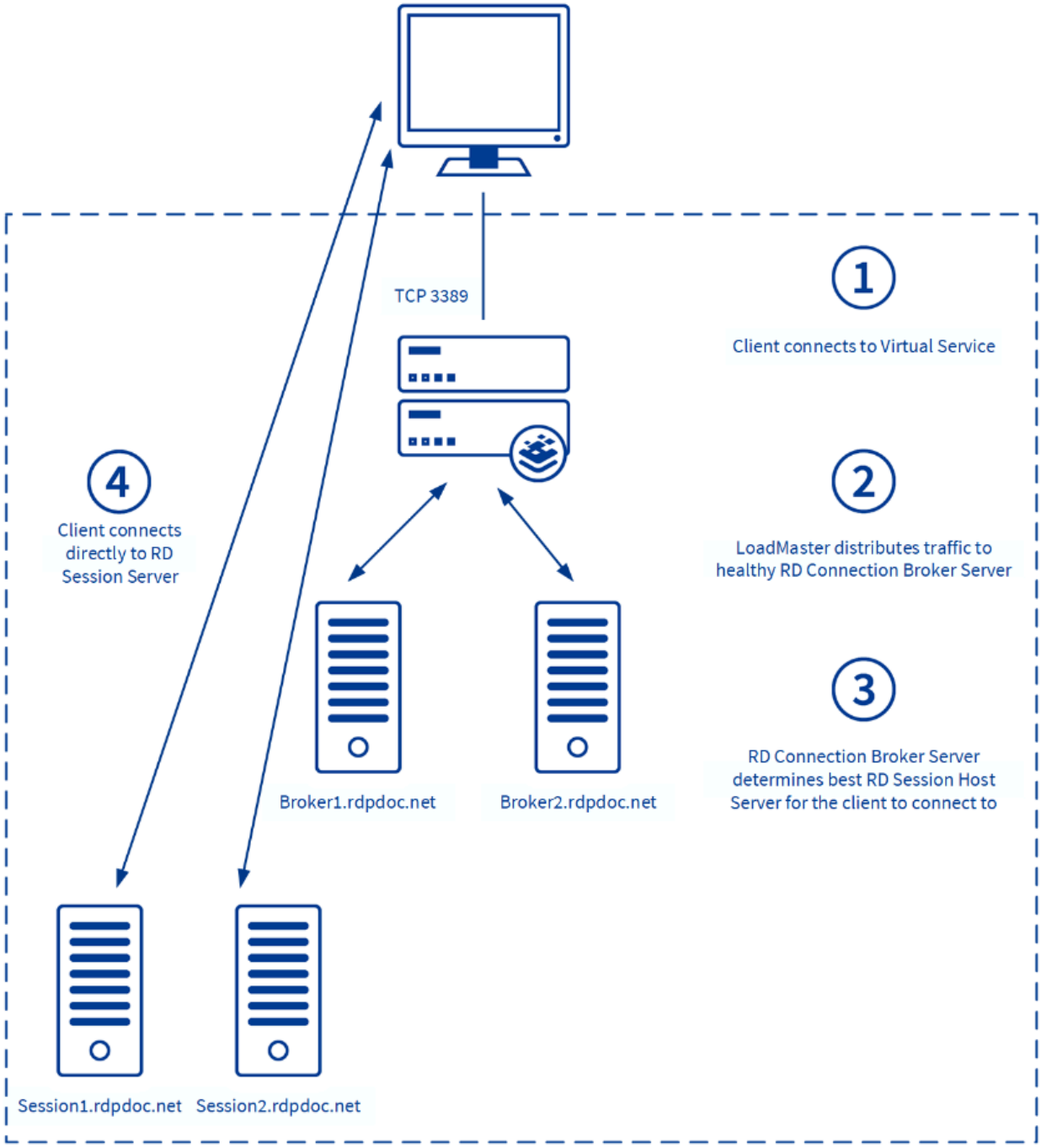
The Microsoft Remote Desktop Connection Broker (RD Connection Broker) role has two responsibilities. First, since Windows Server 2012 the RD Connection Broker role always handles the initial RDP connection and sends the session to the RD Session Host with the least load. Second, the RD Connection Broker makes sure that users are able to reconnect to an existing (disconnected) session. Since Windows Server

2012, end users connecting to the environment always make an initial RDP connection to the RD Connection Broker. The RD Connection Broker then reroutes the user to the RD Session Host server with the least load (based on the load balancing mechanism within the RD Connection Broker) or reroutes the user to an existing (disconnected) session.

RDP traffic running on port 3389 must be load balanced in the LoadMaster.



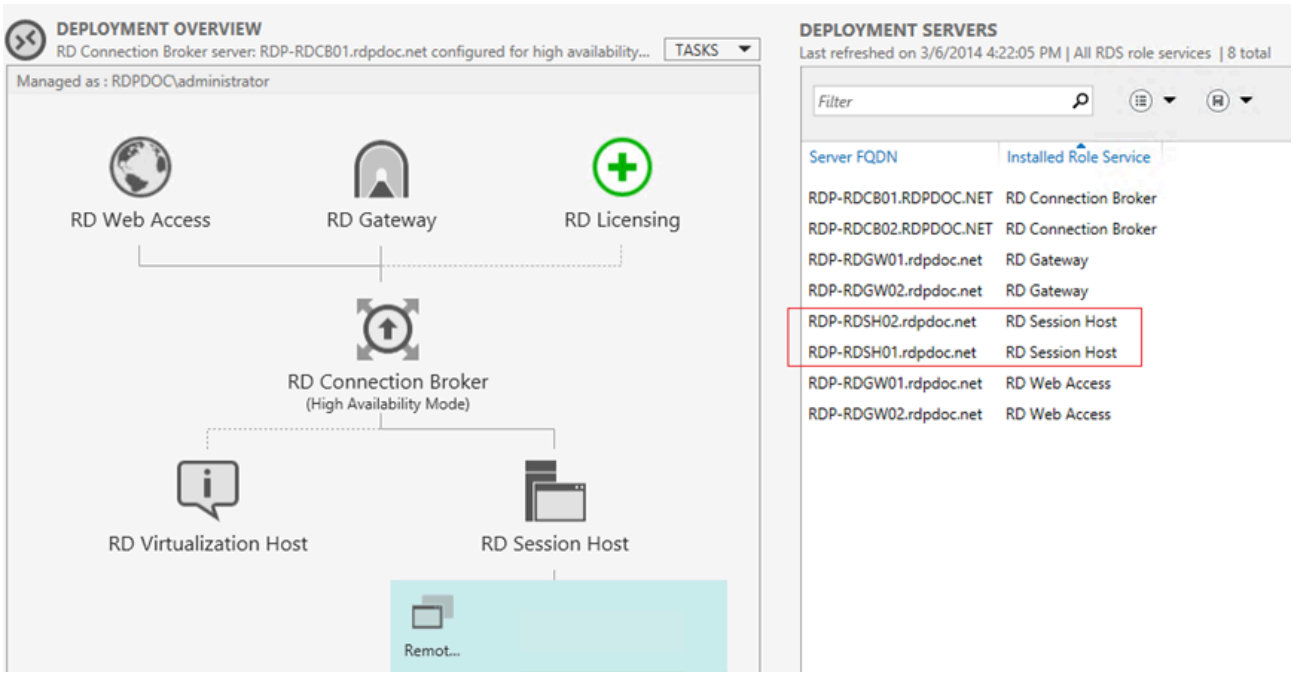
After the RD Connection Broker role is installed, you can use the Remote Desktop Management Services (RDMS) console as part of the Server Manager to retrieve the RD Connection Broker servers as part of the deployment.



Load Balancing Remote Desktop Session Host

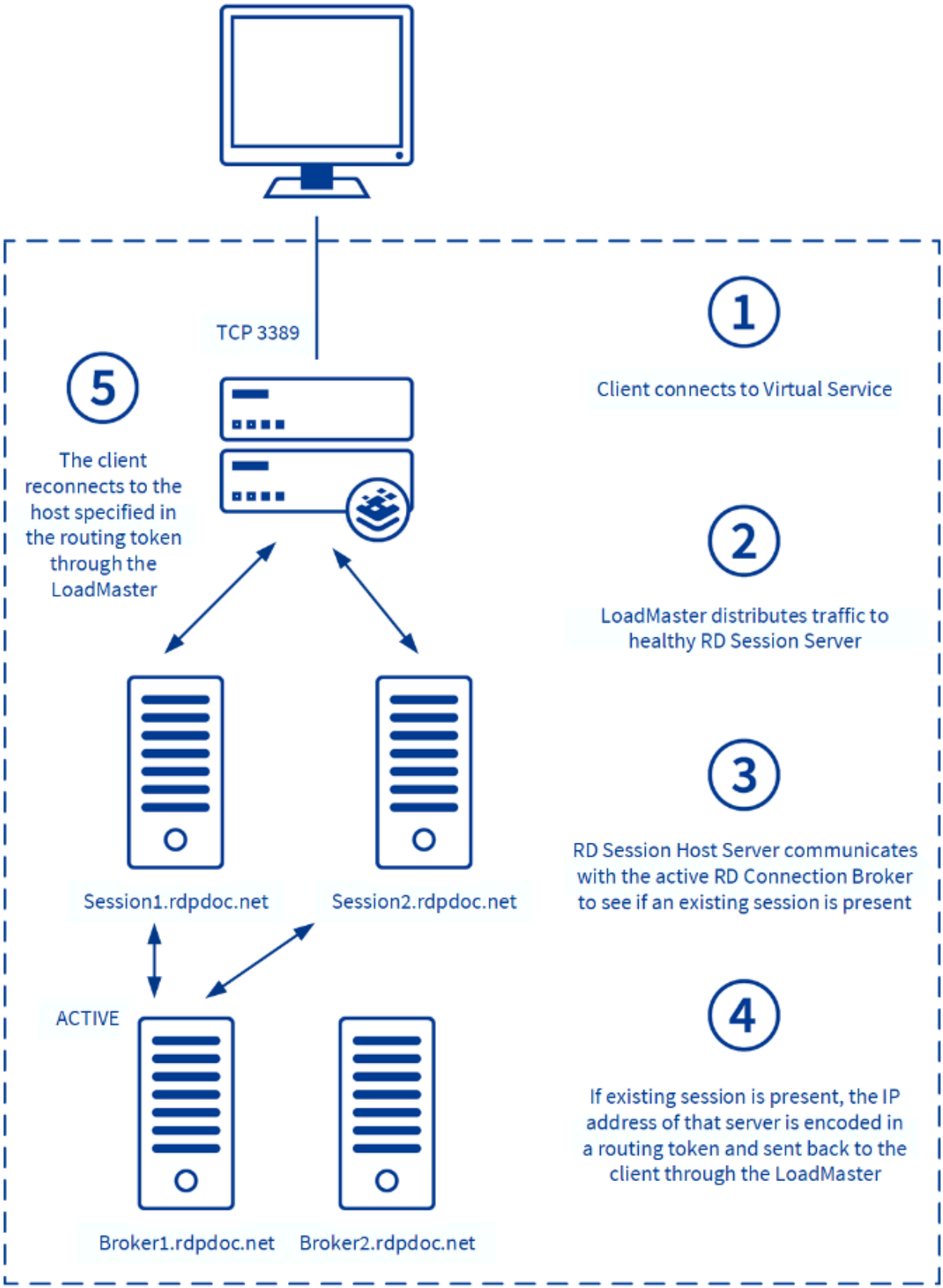
The Microsoft Remote Desktop Session Host (RD Session Host) holds the actual user sessions running the published Remote App or Full Desktop.

RDP traffic running on port 3389 must be load balanced in the LoadMaster. In this scenario, the RD Connection Broker role functionality to redirect to an existing (disconnected) session is still in place, but the RD Connection Broker itself does not actively load balance sessions across RD Session Host servers.



After the RD Session Host role is installed, you can use the Remote Desktop Management Services (RDMS) console as part of the Server Manager to retrieve the RD Session Host servers as part of the deployment.

Note: Note that when load balancing the Session Hosts and using the Connection Broker, you must disable Connection Broker load balancing using Group Policy. You can view the required steps in the Implementing Remote Desktop Session Host Load Balancing section.


TCP 3389
1
Client connects to Virtual Service
2
LoadMaster distributes traffic to healthy RD Session Server
3
RD Session Host Server communicates with the active RD Connection Broker to see if an existing session is present
4
If existing session is present, the IP address of that server is encoded in a routing token and sent back to the client through the LoadMaster
5
The client reconnects to the host specified in the routing token through the LoadMaster
Session1.rdpdoc.net
Session2.rdpdoc.net
ACTIVE
Broker1.rdpdoc.net
Broker2.rdpdoc.net

Deploying the Scenarios

Refer to the following sections for details on deploying the scenarios explained in earlier sections.

Template

Progress Kemp has developed a template containing our recommended settings for this workload. You can install this template to help create Virtual Services (VSs) because it automatically populates the settings. You can use the template to easily create the required VSs with the recommended settings. For some workloads, additional manual steps may be required such as assigning a certificate or applying port following. These steps are covered in the document, if needed.

You can remove templates after use and this will not affect deployed services. If needed, you can make changes to any of the VS settings after using the template.

Download released templates from the following page: LoadMaster Templates.

For more information and steps on how to import and use templates, refer to the Virtual Services and Templates, Feature Description.

Prerequisites

Several prerequisites are listed in the sections below.

Install an SSL Certificate on the LoadMaster

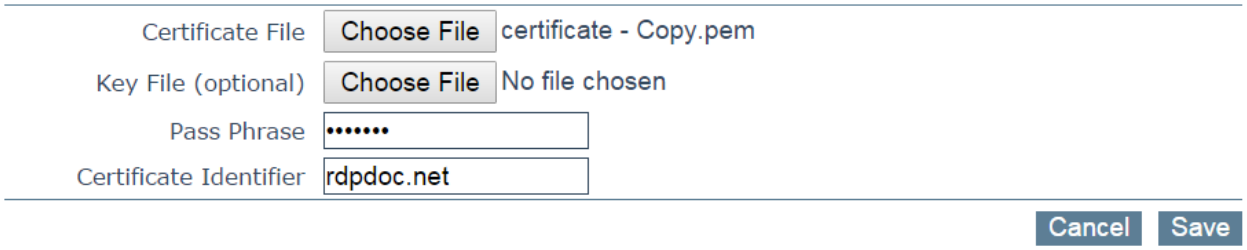
An SSL certificate must be installed on the LoadMaster for some of the services being load balanced. Before you import the certificate, make sure you have it available to the user who manages the LoadMaster. The certificate must match the hostname which is used to connect to the load balanced services of the LoadMaster. The hostname can be a single wildcard, for example, *.domain.com, or multiple regular certificates, for example, rdweb.domain.com.

To install an SSL certificate on the LoadMaster, follow the steps below in the LoadMaster Web User Interface (WUI):

1. In the main menu, select **Certificates & Security > SSL Certificates**.



2. Click **Import Certificate**.



3. Click **Choose File**.
4. Browse to and select the certificate.
5. Enter a **Pass Phrase** if needed.
6. Enter a name (preferably the DNS name of the service) in the **Certificate Identifier** field.
7. Click **Save** then click **OK**.

This certificate is assigned to some of the Virtual Services in later steps.



It is also possible to use this certificate for administrative purposes (browsing the LoadMaster WUI). To do this, on the **Manage Certificates** screen, select the certificate in the **Administrative Certificates** drop-down list and click **Use Certificate**.

Disable Options on the Real Servers

Disable the following two options on the Real Servers:

- Use IP Address Redirection
- Use RD Connection Broker load balancing

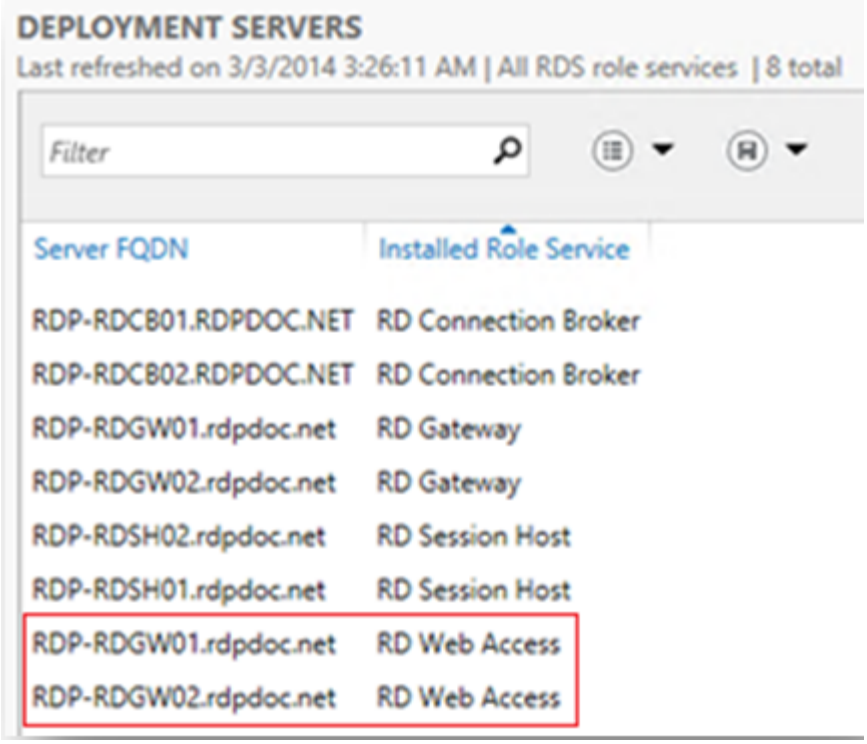
Implementing Remote Desktop Web Access Load Balancing

To configure load balancing for the Remote Desktop Web Access, refer to the following sections.

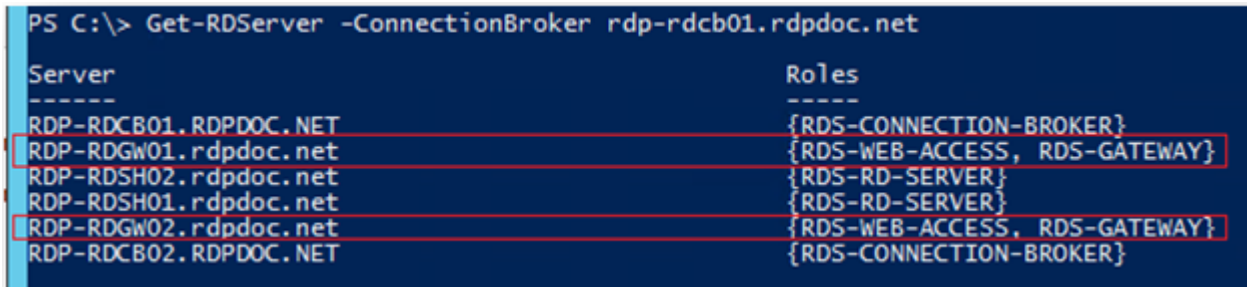
Prerequisites

As discussed in the Load Balancing Remote Desktop Web Access section, implementing load balancing for RD Web Access can be compared with a regular website running on the HTTPS protocol (port 443).

Before configuring the LoadMaster, ensure to have the DNS names and IP addresses available for all Web Servers running the RD Web Access role in your deployment.



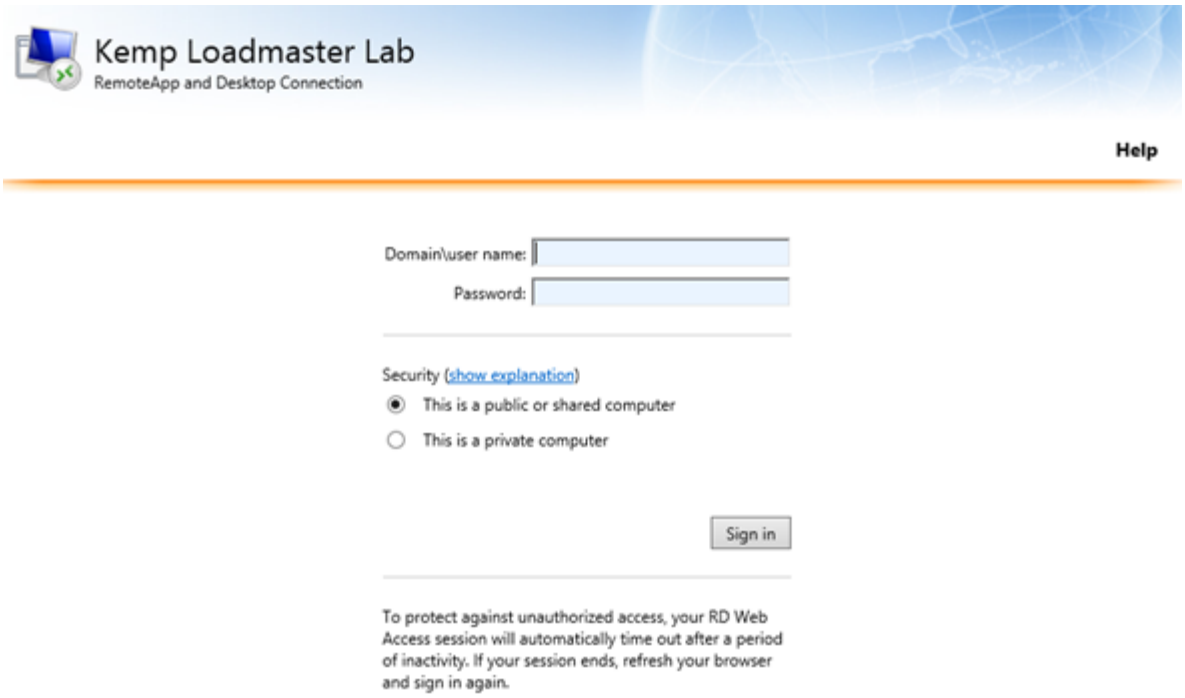
To retrieve the RD Web Access servers in your deployment, open the Remote Desktop Management Services (RDMS) console as part of server manager, go to the **Overview**, and refer to the **Deployment Servers** section as shown above.



Alternatively, use the PowerShell equivalent by running the command **GET-RDServer** as part of the Remote Desktop PowerShell module.

RD Web Access Server	IP Address
RDP-RDGW01.rdpdoc.net	10.154.201.2
RDP-RDGW01.rdpdoc.net	10.154.201.3

In the above example, two RD Web Access servers are part of this deployment.



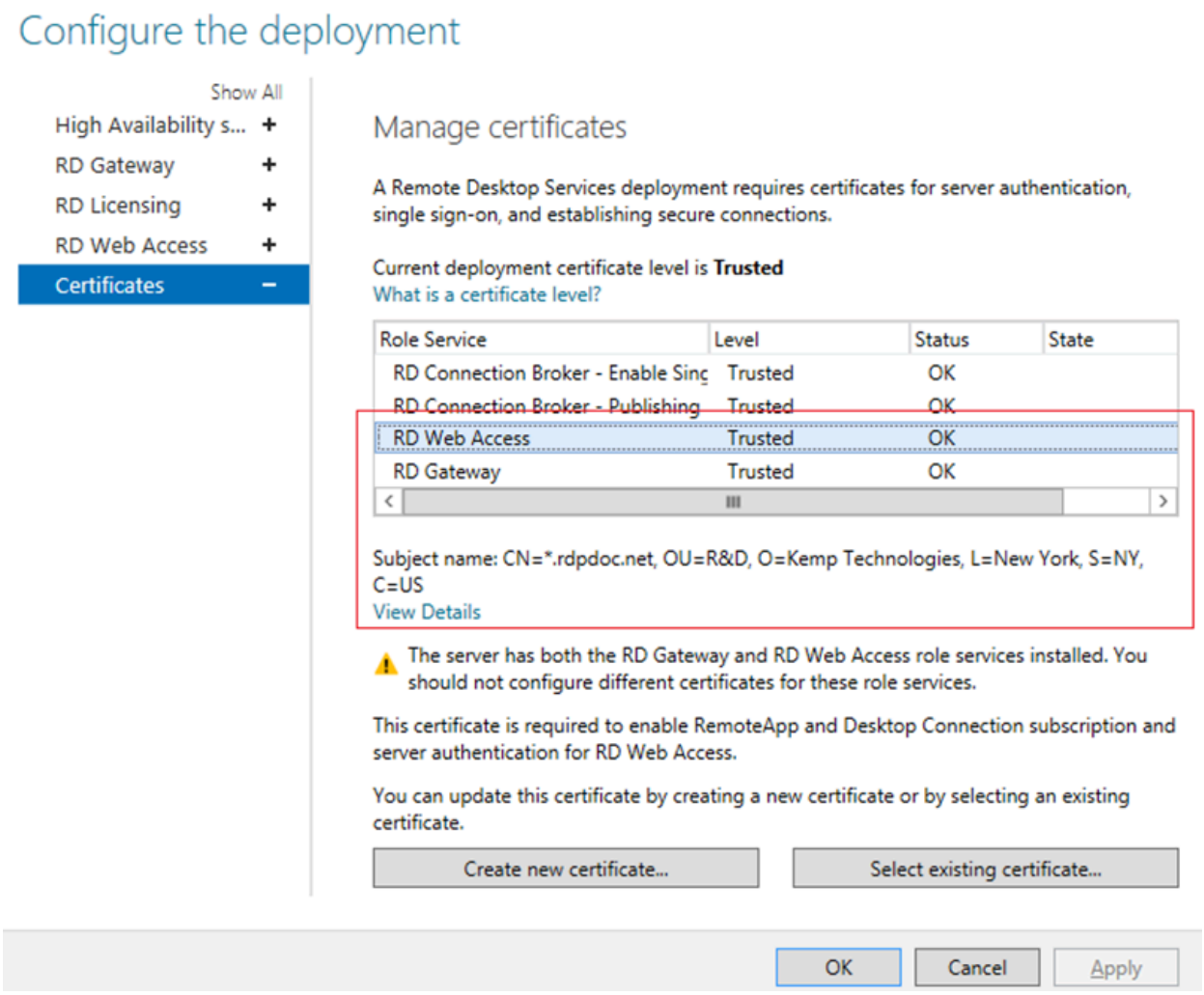
Ensure that all RD Web Access servers are accessible. This can be done by opening a web browser and browsing to each of the individual web servers, for example, **https://RDP-RDGW01.rdpdoc.net/rdweb**.

Load Balanced DNS Name	Load Balanced IP Address
rdpweb.rdpdoc.net	10.154.11.51

Also, ensure you have an IP address and DNS available that is used to access the load-balanced RD Web Access environment. In our example, the above information was used.

Ensure that a valid SSL certificate is configured within the RDS deployment which is trusted by the endpoints that is accessing the RD Web Access environment. The SSL certificate can be centrally configured by following the steps below:

1. Open the Remote Desktop Management Services (RDMS) console.
2. Open **Collections** and select **Tasks**.
3. Click **Edit Deployment Properties**.

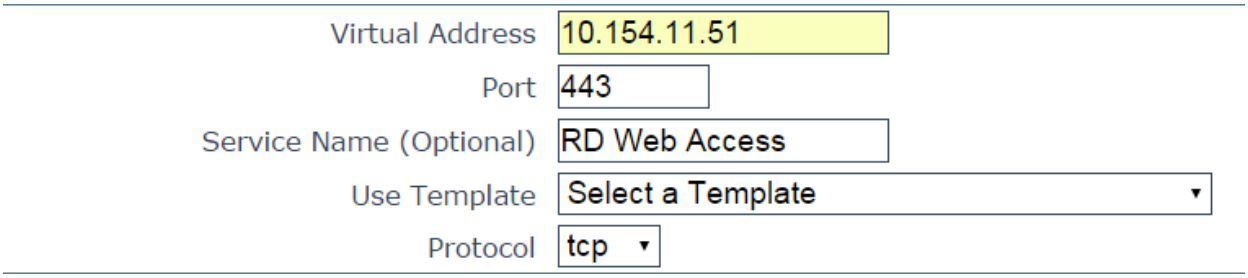


4. Select the **Certificates** tab.
5. Ensure a valid certificate is selected and (if needed) create a new certificate or select a different certificate.

Implementation

Configure the LoadMaster settings by following the steps below in the LoadMaster WUI:

1. In the main menu, select **Virtual Services** and **Add New**.



2. Enter the relevant IP address in the **Virtual Address** text box.

3. Enter **443** as the **Port**.
4. Enter a recognizable **Service Name**, such as **RD Web Access**.
5. Click **Add this Virtual Service**.

Section	Option	Value	Comment
Standard Options	Transparency	Disabled	
	Persistence Method	Source IP Address	
	Scheduling Method	least connection	
	Idle Connection Timeout	660	
SSL Properties	SSL Acceleration	Enabled Reencrypt	A wildcard certificate allows secure connections to be established with a request URL in the format of *.example.com. With this approach, a single certificate secures traffic for all clients in a multi-tenant environment.
	Reencrypt	Enabled	
	Supported Protocols	TLS1.0 TLS1.1 TLS1.2 TLS1.3	While this workload may not support TLS1.3 yet, we recommend enabling it for future proofing.
	Cipher Set	Best Practices	For further information on cipher sets, refer to the **SSL Accelerated Services, Feature Description** on the Documentation page.

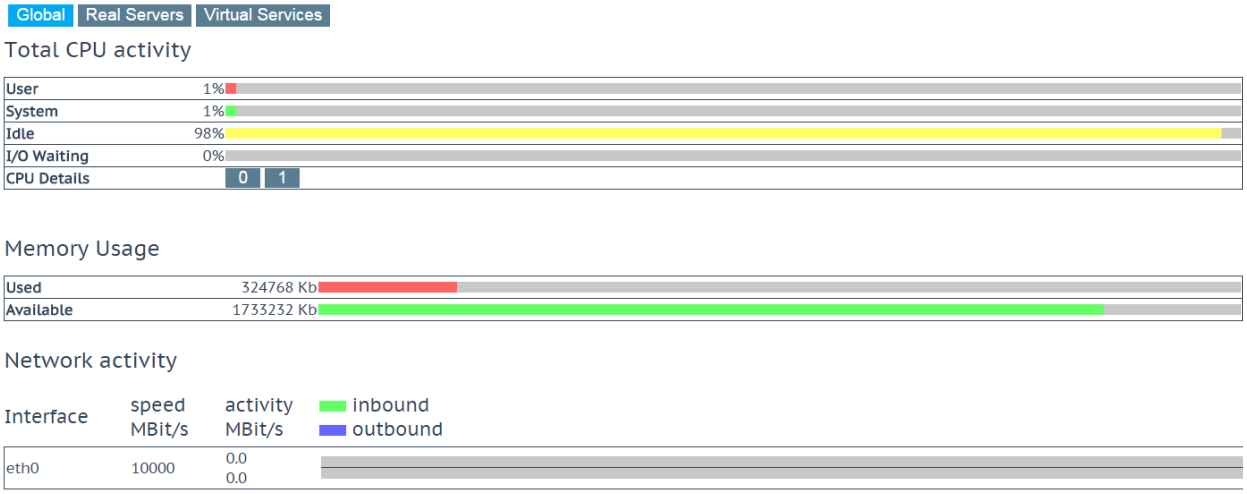
Section	Option	Value	Comment
Advanced Properties	Content Switching	Disabled	
Real Servers	Real Server Check Parameters	HTTPS Protocol	
	Checked Port	443	
	URL	/rdweb	
	HTTP Method	HEAD	

6. Enter the details as shown in the **Web Access Values** table.
7. Expand the **Real Servers** section.
8. Click **Add This Real Server**.
9. Add all required Real Servers.

Testing

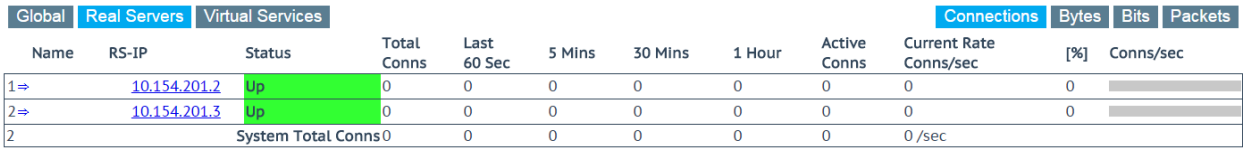
After following the implementation steps in the previous section, follow the steps below to test the load-balanced RD Web Access environment:

1. Open a web browser that is able to reach the load-balanced IP.
2. Browse to the configured DNS name for the load-balanced service, for example, **http://rdp-rdweb.rdpdoc.net/rdweb**. A web page should be presented with the RD Web Access login page. This indicates that the LoadMaster has redirected the session to a Real Server.
3. In the main menu of the LoadMaster WUI, select **Statistics > Real Time Statistics**.

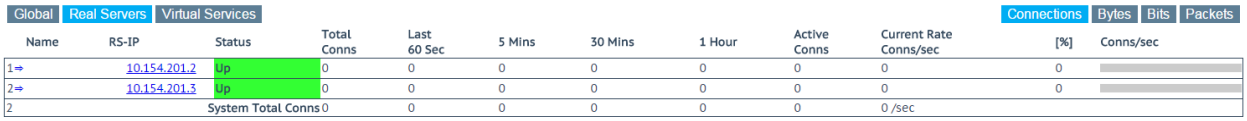


4. Click the **Real Servers** button.

Note: This overview shows the active sessions, sessions over the last hour, in addition to how many requests each Real Server handled.



5. Open another web browser on a different client and perform steps 1 and 2 above.



6. Refresh the LoadMaster statistics page. Notice that, based on the load balancing method we chose, load is spread over both RD Web Access servers.

Implementing Remote Desktop Gateway Load Balancing

To configure load balancing for the Remote Desktop Gateway, refer to the following sections.

Prerequisites

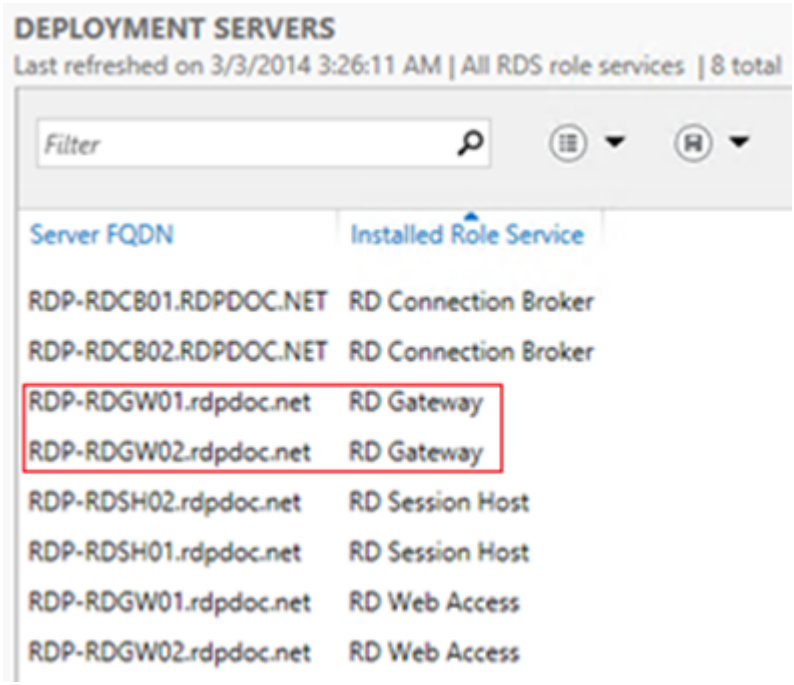
As explained in the Load Balancing Remote Desktop Gateway section, implementing load balancing for RD Gateway is performed by load balancing HTTPS traffic on port 443 and UDP traffic on port 3391.

Before configuring the LoadMaster, ensure to have the DNS names and IP addresses of all servers running the RD Gateway role.

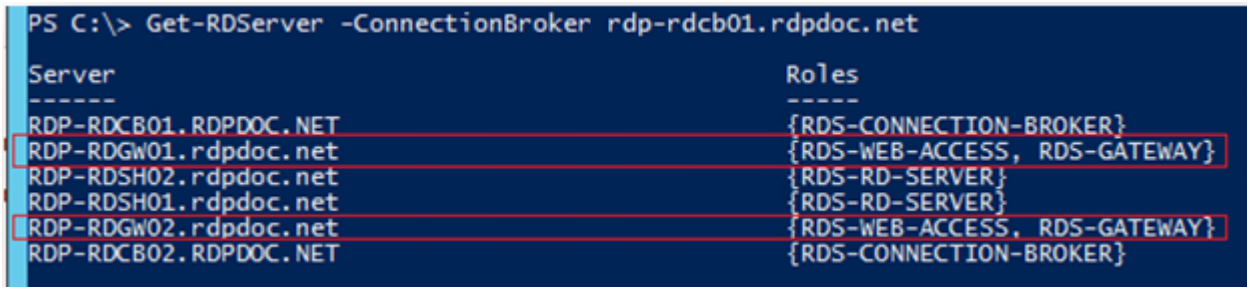
Note: The TLS certificate used on the Virtual Service must be identical to the TLS certificate on the backend RD Gateway Server.

To retrieve the RD Gateway servers in your deployment, follow the steps below:

1. Open the Remote Desktop Management Services (RDMS) console.
2. Open the **Overview**.



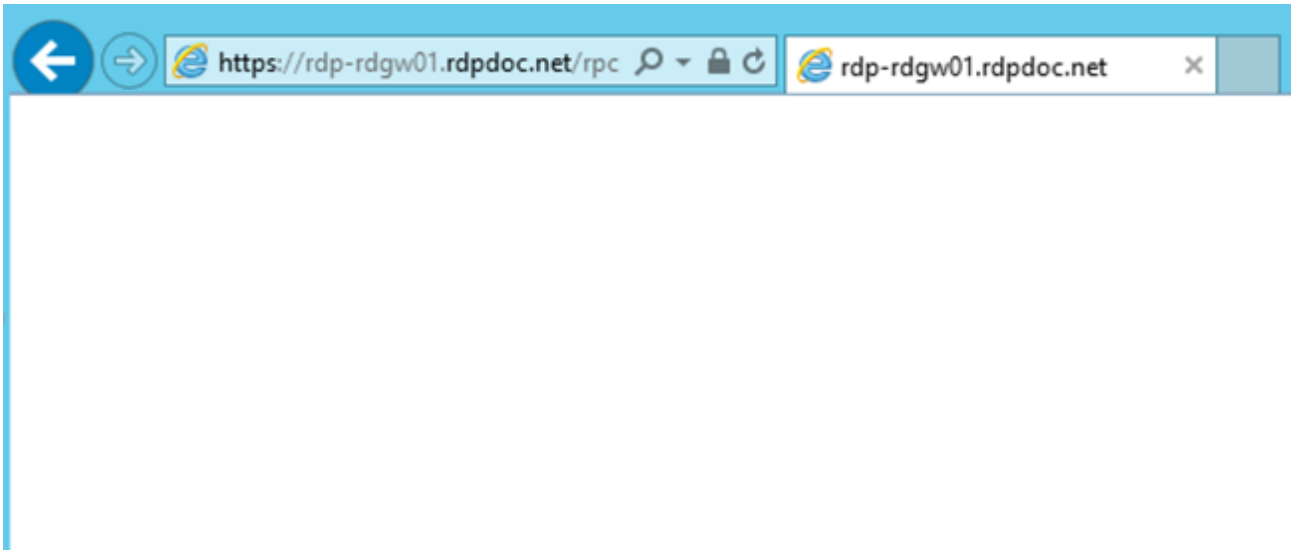
3. Refer to the **Deployment Servers** section.



Alternatively, use the PowerShell equivalent by running the command **GET-RDServer** as part of the Remote Desktop PowerShell module.

RD Web Access Server	IP Address
RDP-RDGW01.rdpdoc.net	10.154.201.2
RDP-RDGW01.rdpdoc.net	10.154.201.3

In the above example, two RD Gateway servers are part of this deployment.



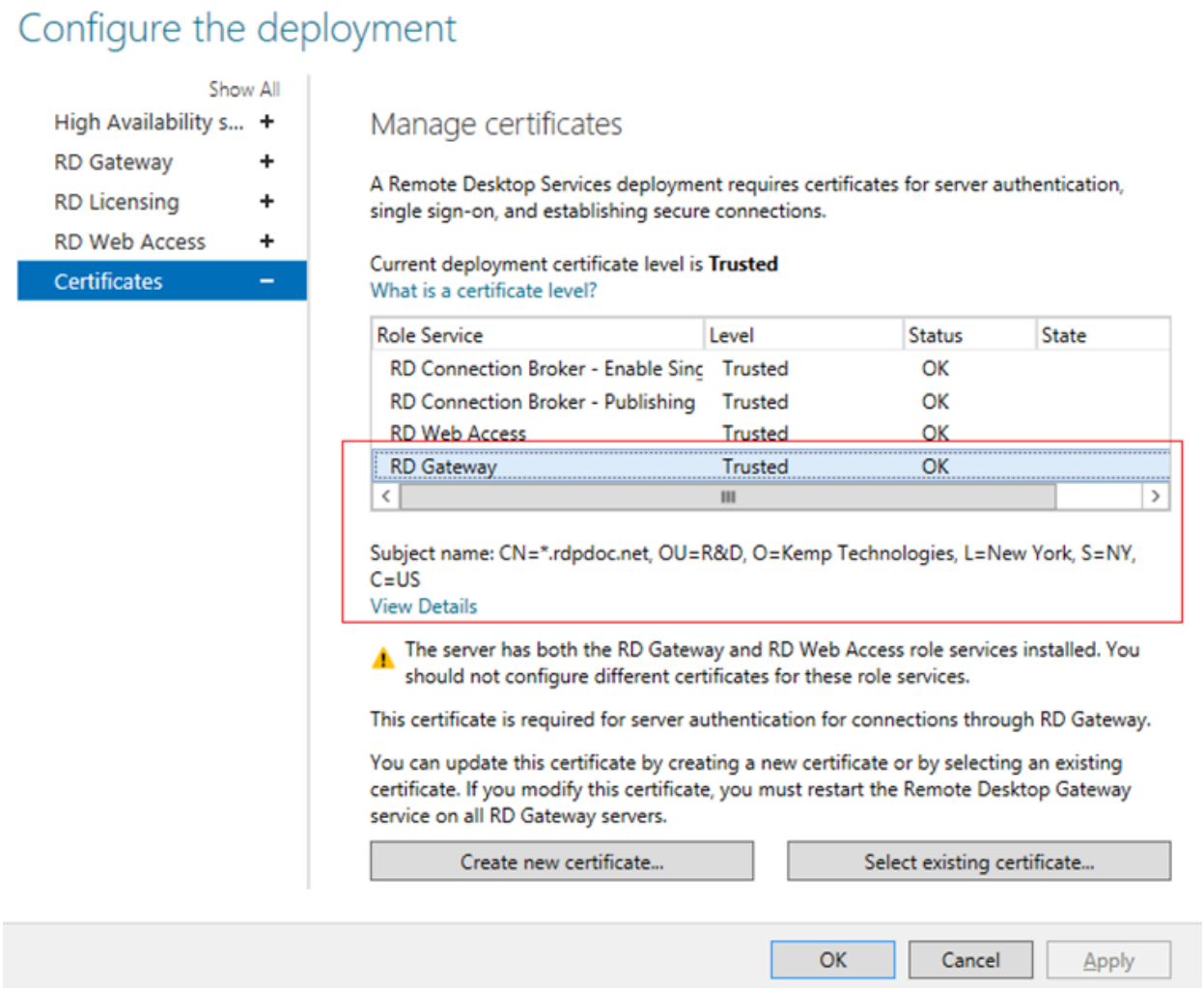
Ensure that all Remote Desktop Gateway servers are accessible. To do this, open a web browser and go to each of the individual web servers, for example, **https://RDP-RDGW01.rdpdoc.net/rpc**. This should bring up an authentication request. After supplying domain credentials, a blank screen should appear. This indicates that the service is reachable.

Load Balanced DNS Name	Load Balanced IP Address
rdgw.rdpdoc.net	10.154.11.52

Also, ensure you have an IP address and DNS available that is used to access the load-balanced RD Web Access environment. In our example, the above information was used.

Ensure that a valid SSL certificate is configured within the RDS deployment which is trusted by the endpoints that are accessing the RD Gateway environment. The SSL certificate can be centrally configured by following the steps below:

1. Open the Remote Desktop Management Services (RDMS) console.
2. Open **Collections** and select **Tasks**.
3. Click **Edit Deployment Properties**.

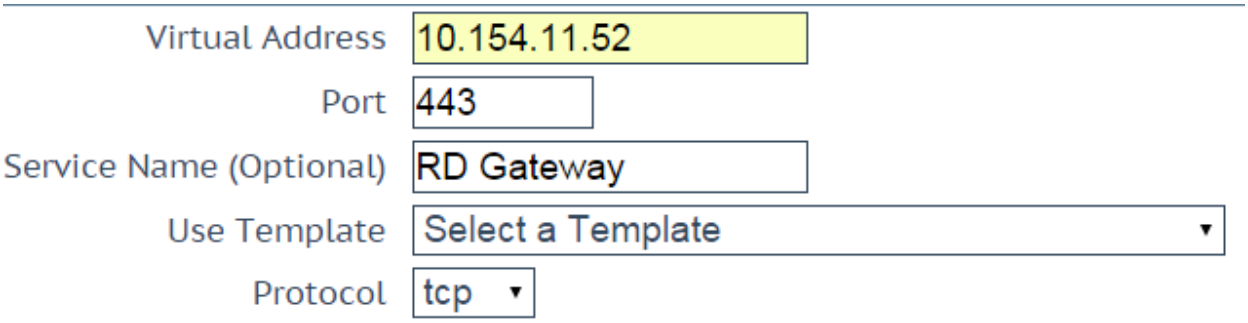


4. Select the **Certificates** tab.
5. Ensure a valid certificate is selected and (if needed) create a new certificate or select a different certificate.

Implementation

Configure the LoadMaster settings by following the steps below in the LoadMaster WUI:

1. In the main menu, select **Virtual Services** and **Add New**.



2. Enter the relevant IP address in the **Virtual Address** text box.
3. Enter **443** as the **Port**.
4. Enter a recognizable **Service Name**, such as **RD Gateway**.
5. Click **Add this Virtual Service**.

Section	Option	Value	Comment
Standard Options	Transparency	Disabled	
	Persistence Mode	Source IP Address	
	Persistence Timeout	1 Hour	
	Scheduling Method	least connection	
	Idle Connection Timeout	28800	8 hours
SSL Properties	SSL Acceleration	Enabled	A wildcard certificate allows secure connections to be established with a request URL in the format of *.example.com. With this approach, a single certificate secures traffic for all clients in a multi-tenant environment.
	Reencrypt	Enabled	
	Supported Protocols	TLS1.0 TLS1.1 TLS1.2 TLS1.3	While this workload may not support TLS1.3 yet, we recommend enabling it for future proofing.
	Cipher Set	Best Practices	For further information on cipher sets, refer to the **SSL Accelerated Services, Feature**

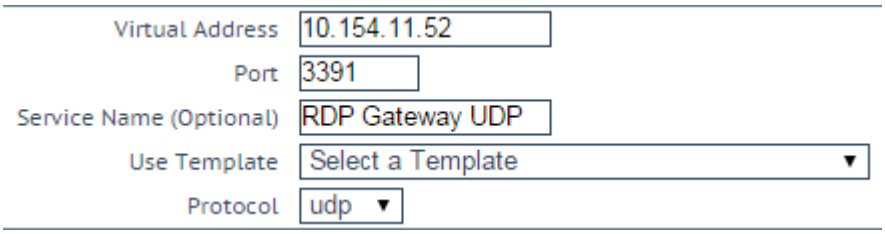
Section	Option	Value	Comment
			Description on the Documentation page.
Advanced Properties	Content Switching	Disabled	
Real Servers	Real Server Check Method	HTTPS Protocol	
	Checked Port	443	
	URL	/rpc	
	HTTP Method	HEAD	

Note: If you are running Remote Desktop Services in the cloud, you must configure the Remote Desktop Gateway to be at Layer 7. In the **Standard Options** section, disable **Layer 4** and ensure **Transparency** is disabled. When you disable **Layer 4** it should set the Real Server **Forwarding method** to **NAT**. These settings are required because the Microsoft Azure or Amazon Web Services (AWS) firewall blocks the traffic when it is directly returned to the client.

6. Enter the settings based on the recommended values above.

   RDP version 8 and above contains new features that use UDP as well as TCP to increase performance over networks with low bandwidth, high latency, or high packet loss. The UDP protocol is also used by the RD Gateway. To allow usage of these protocol enhancements, you must configure the RD Gateway to allow load balancing of UDP traffic. To do this, follow the steps below:

7. In the main menu of the LoadMaster WUI, select **Virtual Services > Add New**.



8. In the **Virtual Address** text box, enter the same IP address that was used in the previous TCP Gateway configuration, for example, **10.154.11.52**.
9. Enter **3391** as the **Port**.

10. Select **udp** as the **Protocol**.
11. Click **Add this Virtual Service**.

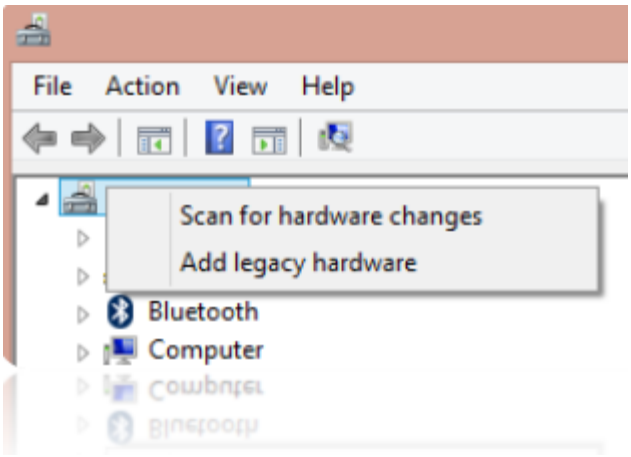
Section	Option	Value	Comment
Standard Options	Transparency	Enabled	
	Persistence Mode	Source IP Address	
	Persistence Timeout	1 Hour	
	Scheduling Method	least connection	In most RD Gateway environments, configuring Least Connection is the most suitable option. However, any option can be selected. For example, if a relative weight is configured to an RD Gateway Server, selecting weighted least connection here would also add the configured weight as a factor in calculating the schedule.
Real Servers	Real Server Check Method	ICMP Ping	
	Port	3391	
	Forwarding Method	Direct return	

12. Enter the settings based on the recommended values above.

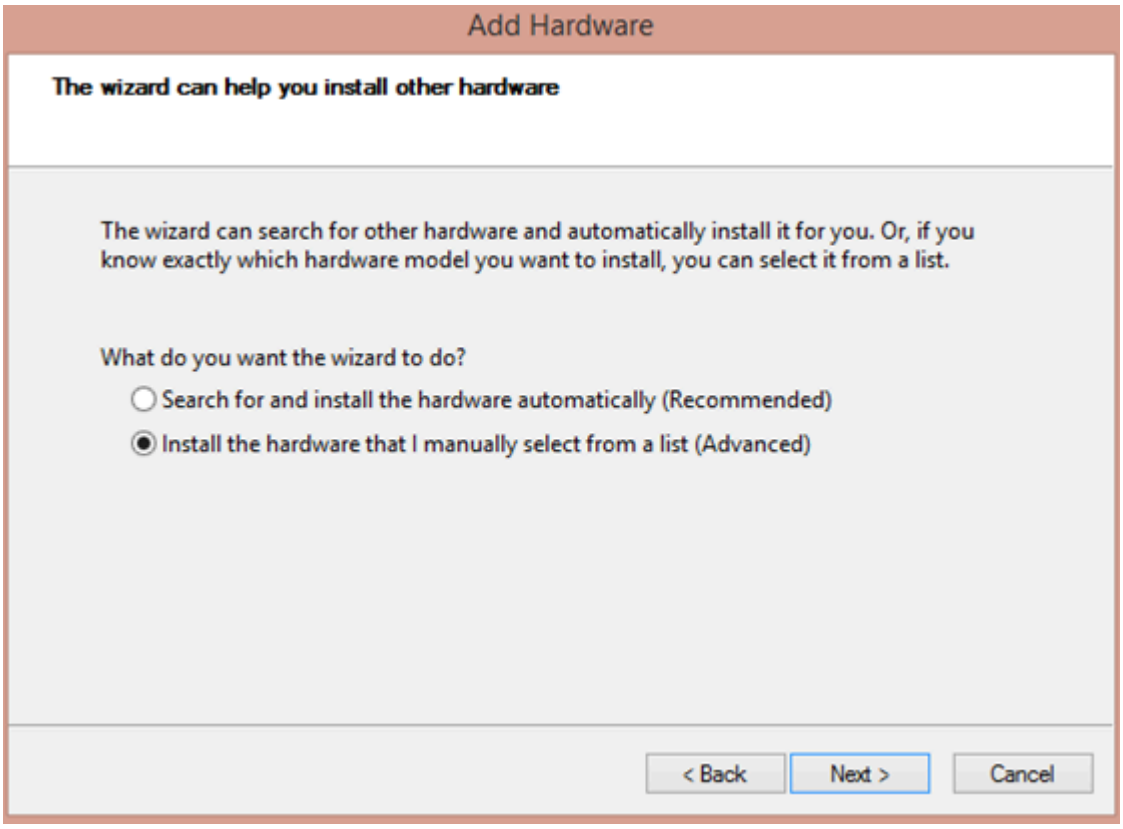
Cloud Deployments – The UDP traffic for RDP version 8 must be set to use Layer 7 when deployed in cloud environments. In the Standard Options section, disable **Transparency** and ensure that the forwarding method is set to **NAT**. These settings are required because the Microsoft Azure or Amazon Web Services (AWS) firewall blocks traffic that is directly returned to the client.

Non-Cloud Deployments -The UDP traffic for RDP version 8 can be configured to use Direct Server Return (DSR). Therefore, you must make some changes to the RD Gateway Servers to make the setup work. To make these changes, follow the steps below:

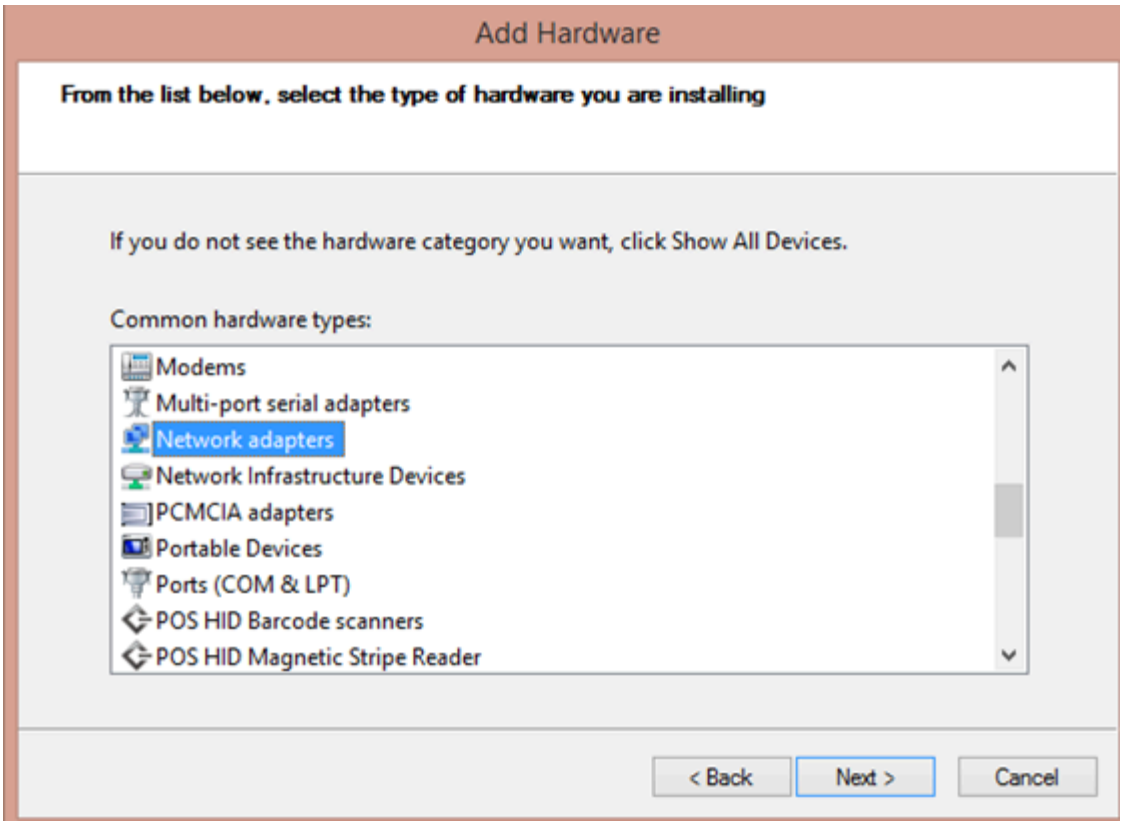
1. Open the **Device Manager** on both RD Gateway Servers.



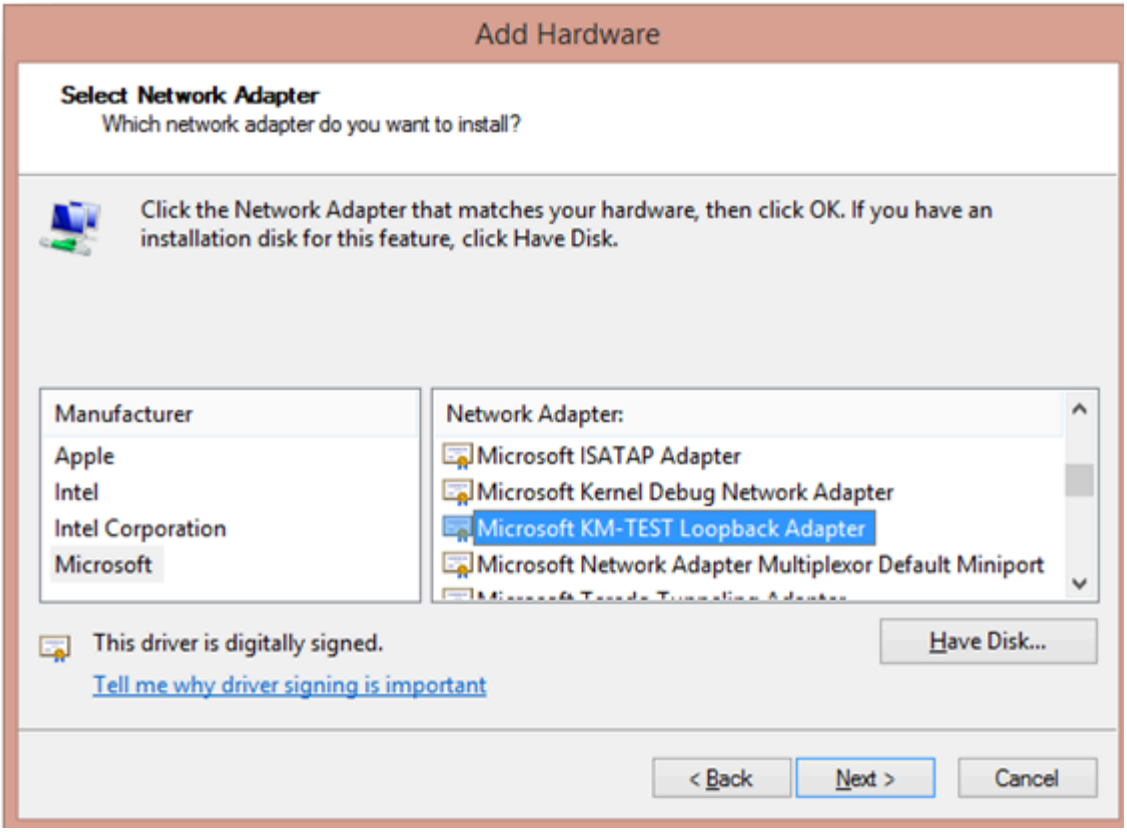
2. Right-click the computer name and select **Add legacy hardware**.



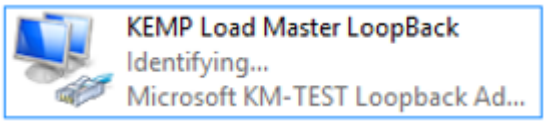
3. Select **Install the hardware that I manually select from a list (Advanced)**.
4. Click **Next**.



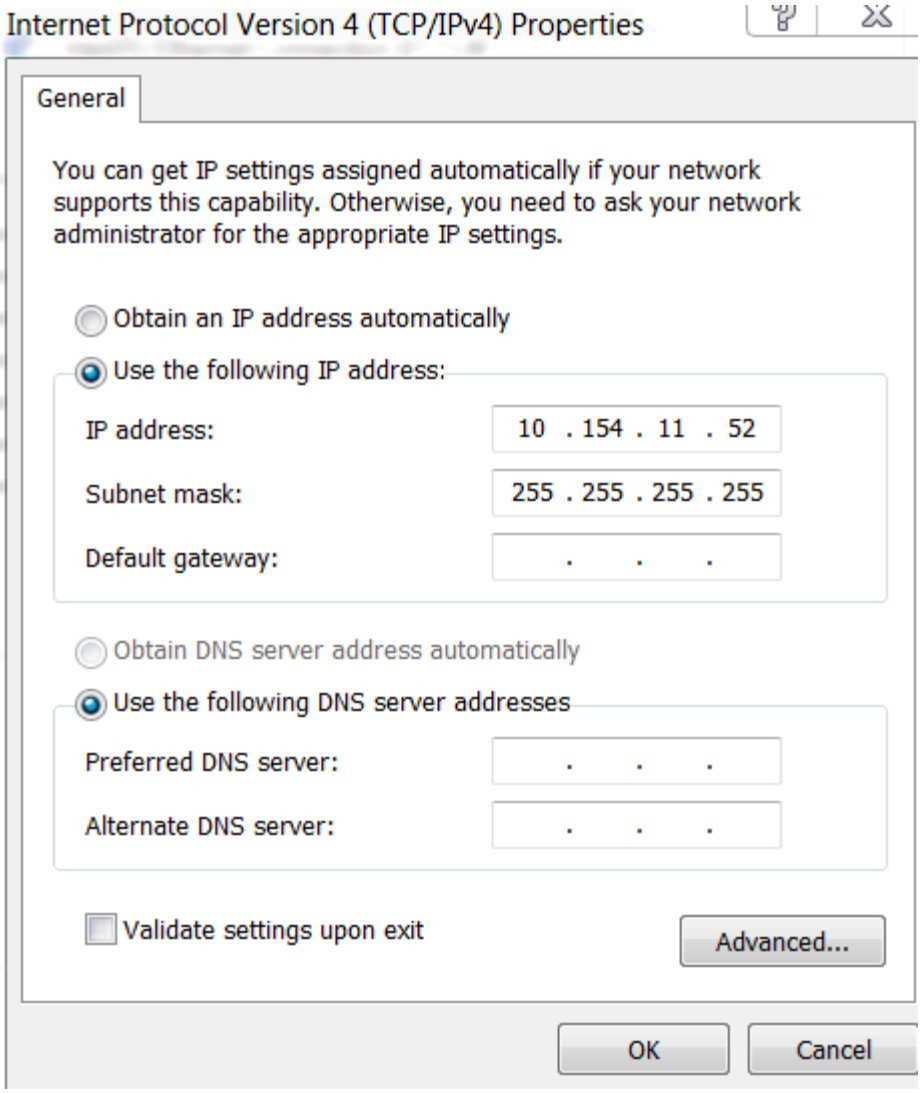
5. Select **Network adapters**.
6. Click **Next**.



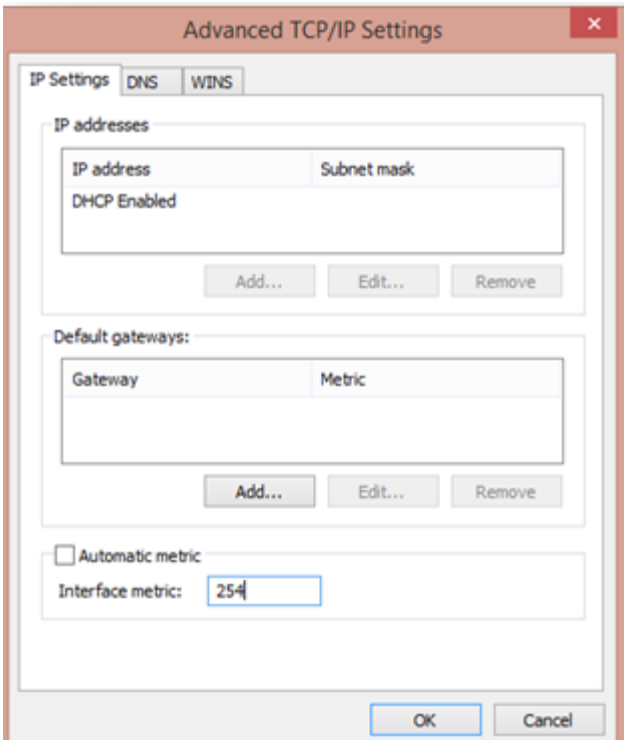
7. Select the **Microsoft KM-TEST Loopback Adapter**.
8. Click **Next**.



9. This creates a new network adapter. To make it easier to identify, rename it, for example to **LoadMaster LoopBack**.
10. Open the TCP/IP properties.



11. In the **IP address** text box, enter the IP address that matches the Virtual Service address.
12. Enter **255.255.255.255** in the **Subnet mask** text box.
13. Click the **Advanced** button.



14. Enter **254** in the **Interface metric** text box.
15. Click **OK**.
16. Click **OK** again.
17. Run the following three commands (using elevated permissions) in the console. Enter the name of the loopback adapter where **<loopback>** is mentioned. Enter the name of the primary network adapter where **<net>** is mentioned.

netsh interface ipv4 set interface <net> weakhostreceive=enabled

netsh interface ipv4 set interface <loopback> weakhostreceive=enabled

netsh interface ipv4 set interface <loopback> weakhostsend=enabled

Testing

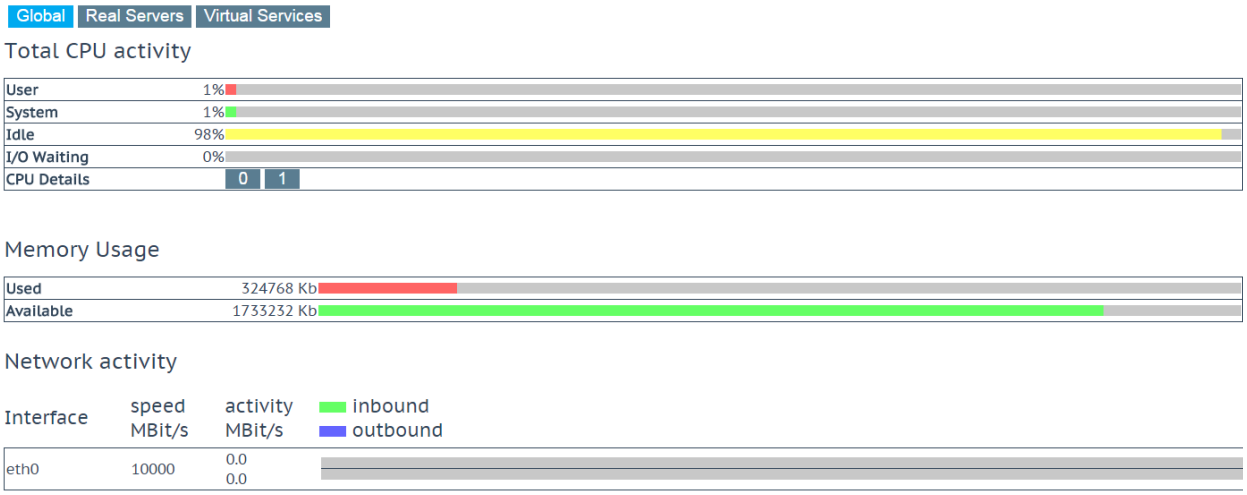
After following the implementation steps in the previous section, follow the steps below to test the load-balanced RD Gateway environment:

1. Open an RDP connection to the RDS 2012 deployment. This can be performed in various ways:
   - Use RD Web Access. Refer to the Load Balancing Remote Desktop Web Access section.
   - Use the Remote App and Desktop Connections (RADC) as part of the Control Panel.
   - Manually create a .RDP file.

   Note: Ensure to leverage the RD gateway. Remember that the RD Gateway can also be configured to be bypassed when a direct RDP connection to the RD Session Hosts is possible. Either test from a

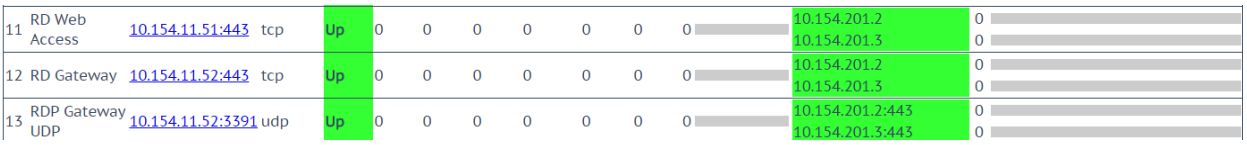
client that you have confirmed is not able to connect to the RD Session Hosts directly, or configure your RDP settings to always use the RD Gateway.

2. After opening a connection, in the main menu of the LoadMaster WUI, select **Statistics**.



3. Click **Virtual Services**.

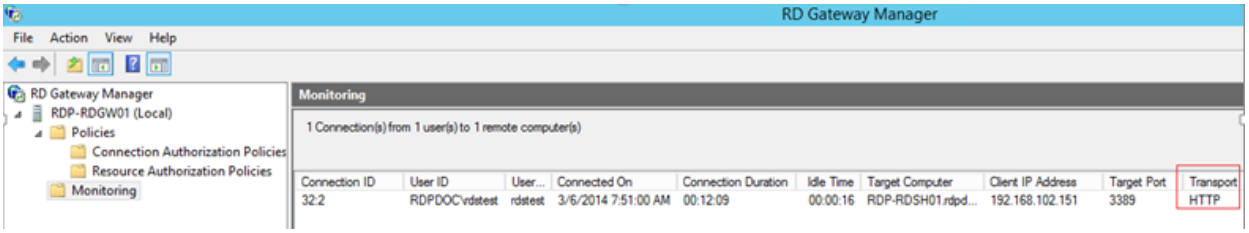
Note: This overview shows the active sessions, sessions over the last hour, in addition to how many requests each Real Server handled.



4. Open another web browser on a different client and perform steps 1 and 2 above.
5. Refresh the LoadMaster statistics page. Notice that, based on the load balancing method selected, load is spread over both RD Gateway servers.

   To ensure that the new HTTP-based transport protocol of the RD Gateway on Windows Server 2012 is being leveraged, follow the steps below:

6. Log in to the RD Gateway Server that holds the active test session.



7. Open **Administrative Tools** and then **Remote Desktop Gateway Manager**.
8. Expand your RD Gateway server and click **Monitoring**.
9. Confirm that your active session uses **HTTP** as the **Transport**, and not **RPC-HTTP**.

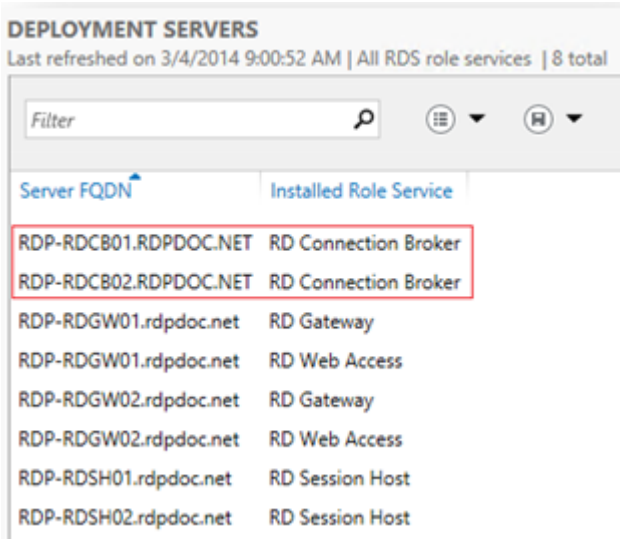
Implementing Remote Desktop Connection Broker Load Balancing

To configure load balancing for the Remote Desktop Connection Broker, refer to the following sections.

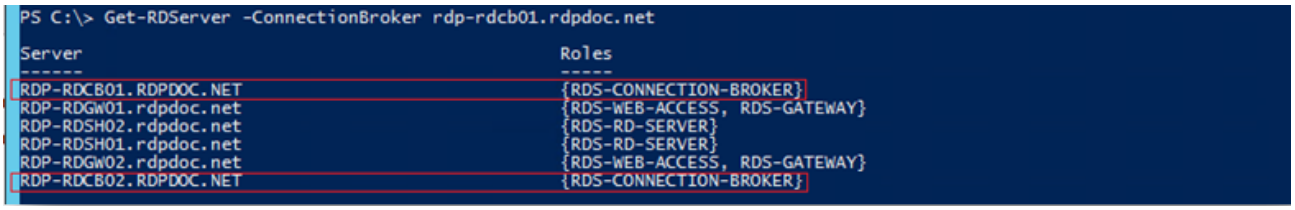
Prerequisites

As discussed in the Load Balancing Remote Desktop Connection Broker section, implementing load balancing for RD Connection Broker is performed by load balancing RDP traffic on port 3389. In this scenario, we load balance the initial sessions that users perform on the RD Connection Broker.

Before configuring the LoadMaster, ensure to have the DNS names and IP addresses available for all Web Servers running the RD Connection Broker role in your deployment.



To retrieve the RD Connection Broker servers in your deployment, open the Remote Desktop Management Services (RDMS) console as part of server manager, go to the **Overview**, and refer to the **Deployment Servers** section as shown above.



Alternatively, use the PowerShell equivalent by running the command **GET-RDServer** as part of the Remote Desktop PowerShell module.

RD Web Access Server	IP Address
RDP-RDCB01.rdpdoc.net	10.154.201.4
RDP-RDCB01.rdpdoc.net	10.154.201.5

In the above example, two RD Connection Broker servers are part of this deployment.

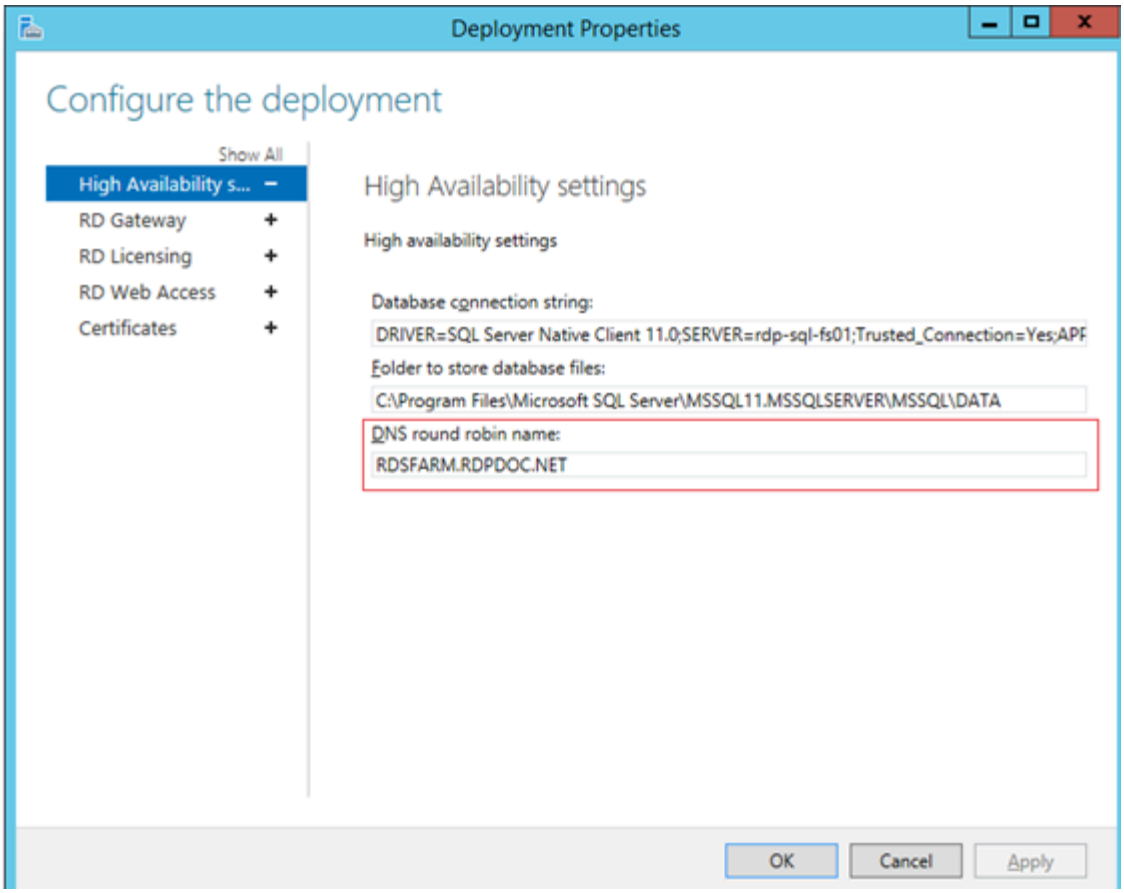
Ensure that all RD Broker servers are accessible on port 3389. This can be done by opening the command line and running the command **telnet <IPAddressOfConnectionBroker> 3389** or use mstsc.exe to open an RDP connection to the RD Connection Broker.

Load Balanced DNS Name	Load Balanced IP Address
rdsfarm.rdpdoc.net	10.154.11.52

Also, ensure you have an IP address and DNS available that are used to access the load balanced RD Connection Broker environment. In our example, the above information was used.

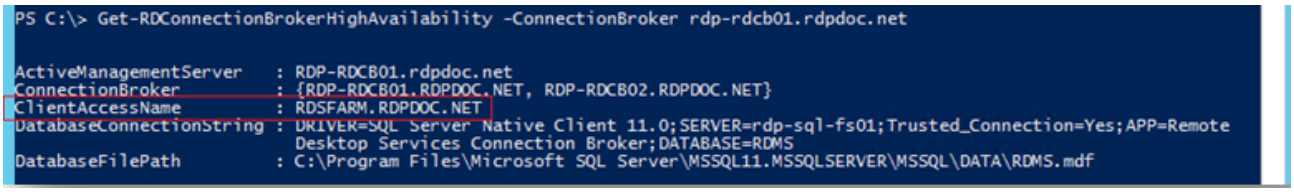
The DNS name must match the DNS Round Robin name as configured in the RDS deployment. To confirm the value, follow the steps below:

1. Open the Remote Desktop Management Services (RDMS) console.
2. Click **Collections**.
3. Select **Tasks**.
4. Click **Edit Deployment Properties.**



5. Select the **High Availability Settings** tab.

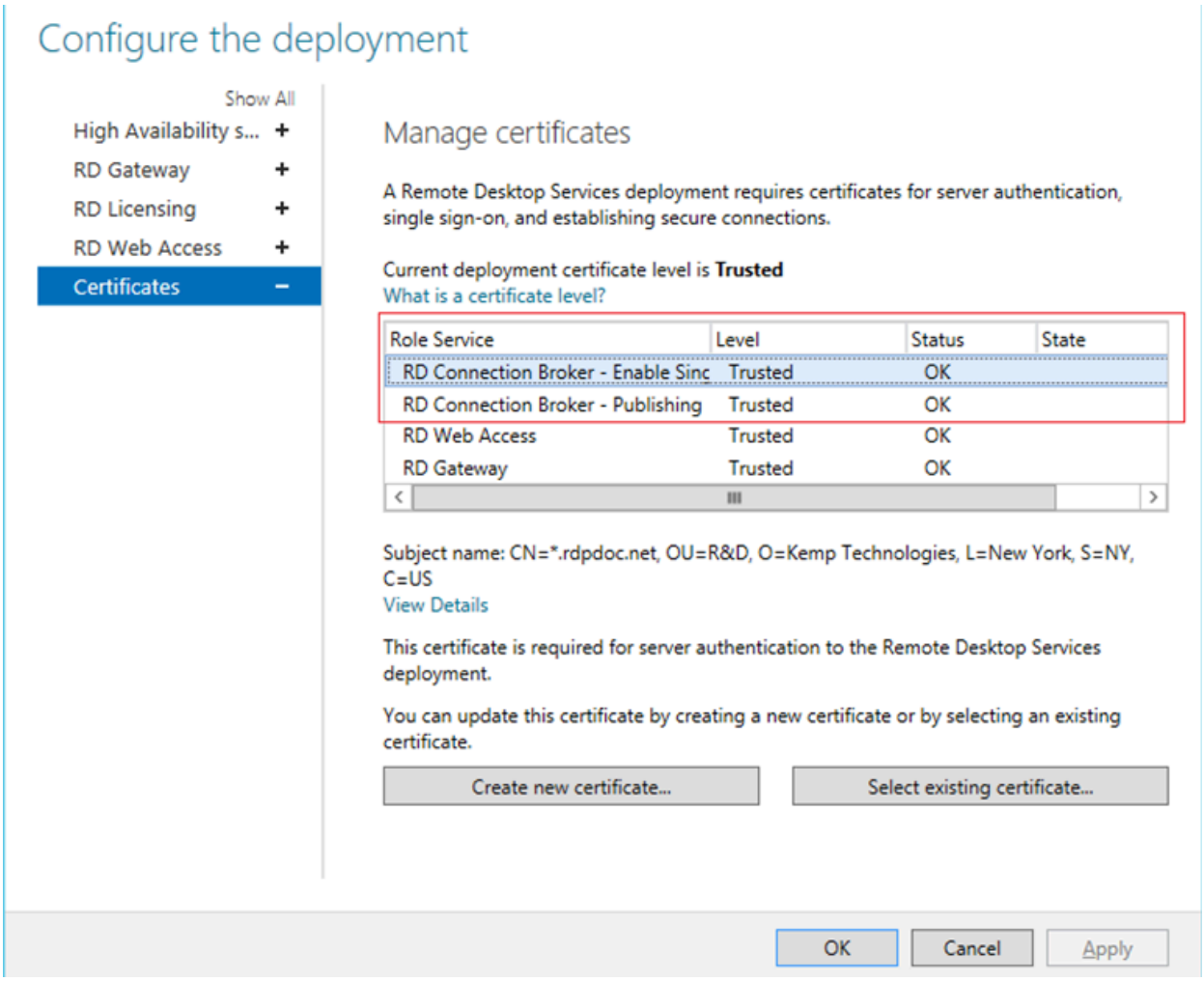
The value is displayed underneath **DNS round robin name**.



Alternatively, use the PowerShell equivalent by running the command **Get-RDConnectionBrokerHighAvailability** in the Remote Desktop PowerShell module.

Ensure that a valid SSL certificate is configured within the RDS deployment which is trusted by the endpoints that is accessing the RD Connection Broker environment. The SSL certificate can be centrally configured by following the steps below:

1. Open the Remote Desktop Management Services (RDMS) console.
2. Open **Collections** and select **Tasks**.
3. Click **Edit Deployment Properties**.

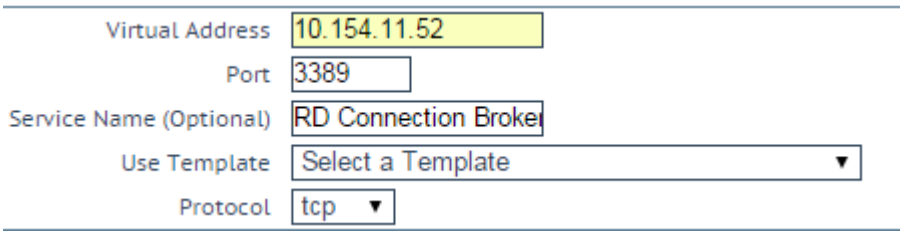


4. Select the **Certificates** tab.
5. Ensure a valid certificate is selected and (if needed) create a new certificate or select a different certificate.

Implementation

Configure the LoadMaster settings by following the steps below in the LoadMaster WUI:

1. In the main menu, select **Virtual Services** and **Add New**.



2. Enter the relevant IP address in the **Virtual Address** text box.

Note: In our example the IP address is **10.154.11.52**.

3. Enter **3389** as the **Port**.
4. Enter a recognizable **Service Name**, such as **RD Connection Broker**.
5. Click **Add this Virtual Service**.

Section	Option	Value	Comment
Standard Options	Transparency	Disabled	
	Persistence Mode	Terminal Service or Source IP Address	In the **Standard Options** section, a **Persistence Mode** can be specified. The RD Connection Broker role itself does not rely on persistence. This is because the RD Connection Broker servers only handle the initial RDP request, it does not contain any active sessions. Therefore, the persistence mode can be left to the default option.
	Persistence Timeout	1 Hour	
	Scheduling Method	least connection	In most RD Connection Broker environments, configuring **least connection** is the most suitable option. However, any option can be selected. For example, if a relative weight is configured to an RD Connection Broker server, selecting **weighted least connection** here would also add the configured weight as a factor in calculating the schedule.
	Idle Connection Timeout	660	

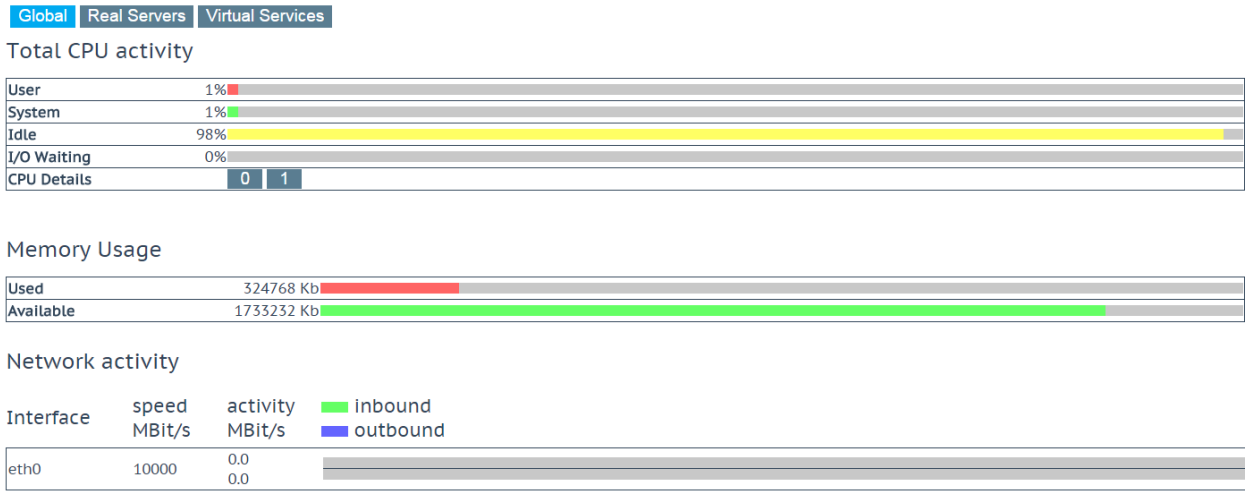
Section	Option	Value	Comment
Real Servers	Real Server Check Method	Remote Terminal Protocol	
	Checked Port	3389	
	Forwarding method	Nat	

6. Enter the settings based on the recommended values above.

Testing

After following the implementation steps in the previous section, follow the steps below to test the load balanced RD Connection Broker environment:

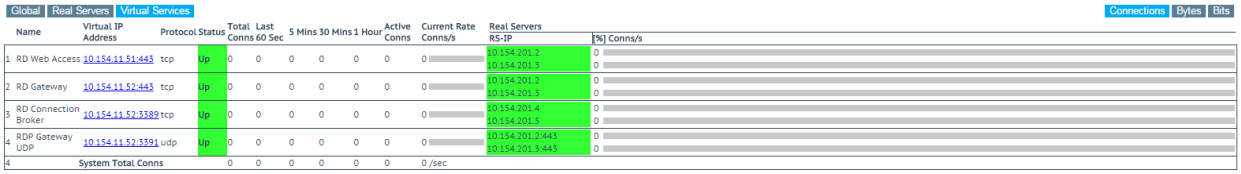
1. Open an RDP connection to the RDS 2012 deployment. This can be performed in various ways:
   - Use RD Web Access. Refer to the Load Balancing Remote Desktop Web Access section.
   - Use the Remote App and Desktop Connections (RADC) as part of the Control Panel.
   - Manually create a .RDP file.
2. In the main menu of the LoadMaster WUI, select **Statistics**.



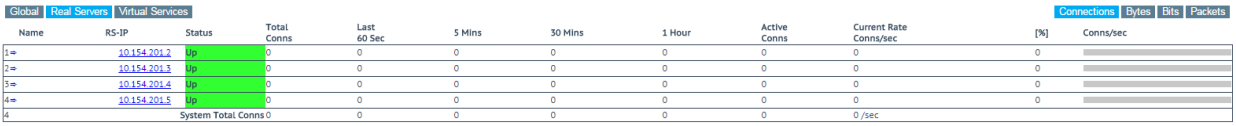
3. Click **Virtual Services**.

Note: This overview shows the active sessions, sessions over the last hour, in addition to how many requests each Real Server handled. As explained, because the RD Connection Broker Real Servers only

handle the initial RDP connection, you will likely never see any active sessions because as soon as the RD Connection Broker has referred the user to an RD Session Host, the connection from the client to the RD Connection Broker is dropped as the client now has a connection with the RD Session Host itself.



4. Open another web browser on a different client and perform steps 1 and 2 above.



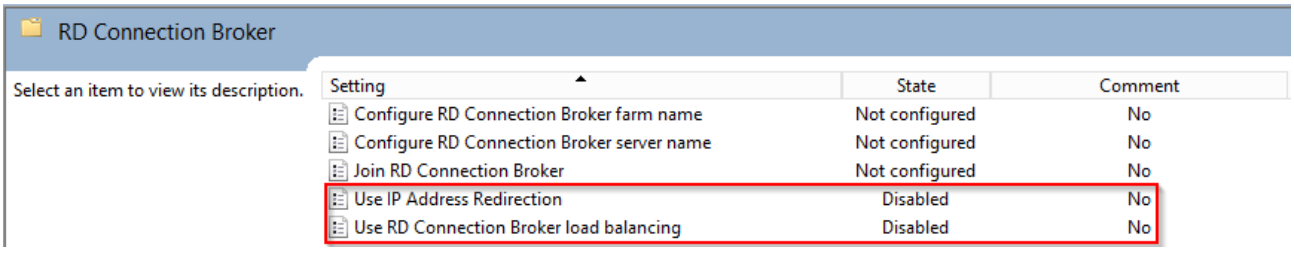
5. Refresh the LoadMaster statistics page. Notice that, based on the load balancing method we chose, load is spread over both RD Connection Broker servers.

Implementing Remote Desktop Session Host Load Balancing

To configure load balancing for the Remote Desktop Session Host, refer to the following sections.

Prerequisites

As discussed in the Load Balancing Remote Desktop Session Host section, implementing load balancing for RD Session Host is performed by load balancing RDP traffic on port 3389. In essence, the LoadMaster replaces the load balancing options that come with the Microsoft RD Connection Broker. It is important to realize that starting from Windows Server 2012, in most cases, Remote Desktop Services is deployed using the Scenario-Based Deployment as part of the Server Managed in Windows Server 2012. In these cases, you automatically get an RD Connection Broker as part of your deployment. This RD Connection Broker automatically starts load balancing sessions for the RD Session Host servers in your deployment. You will want to avoid this because it will result in double load balancing.



To disable RD Connection Broker Load balancing and Use IP Address Redirection, create a Group Policy Object on the OU where your RD Session Host servers are located and set the following GPO to disabled:

Computer Configuration\Policies\Administrative Templates\Windows Components\Remote Desktop Services\Remote Desktop Session Host\RD Connection Broker\Use IP Address Redirection

Computer Configuration\Policies\Administrative Templates\Windows Components\Remote Desktop

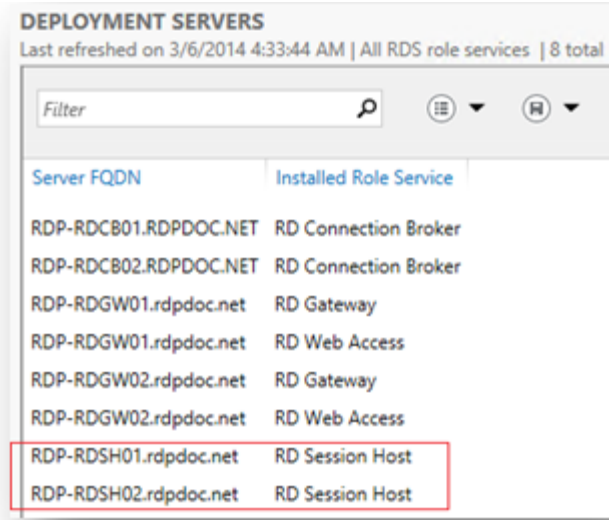
Services\Remote Desktop Session Host\RD Connection Broker\User RD Connection Broker load balancing

Disabling these options does not prevent the RD Connection Broker from allowing users to reconnect to an existing session. That functionality still operates.

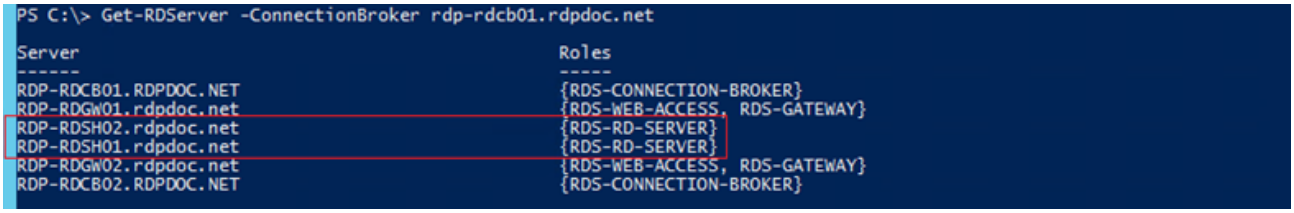
Besides the Scenario-Based Deployment in Server Manager, you could also use the Role-Based Deployment and only deploy the RD Session Host servers. This would result in a set of RD Session Host servers without an RD Connection Broker, and thus the above GPO setting would not be needed.

Note: Note that this approach leads to an environment where you cannot manage the RDS environment using the Server Manager Graphical User Interface (GUI). You would be fully dependent on GPO, Windows Management Instrumentation (WMI), and registry settings to manage your environment.

Before configuring the LoadMaster, ensure to have the DNS names and IP addresses available for all Web Servers running the RD Session Host role.



To retrieve the RD Session Host servers in your deployment, open the Remote Desktop Management Services (RDMS) console as part of server manager, go to the **Overview** and refer to the **Deployment Servers** section as shown above.



Alternatively, use the PowerShell equivalent by running the command **GET-RDServer** as part of the Remote Desktop PowerShell module.

RD Web Access Server	IP Address
RDP-RDSH01.rdpdoc.net	10.154.201.6
RDP-RDSH02.rdpdoc.net	10.154.201.7

In the above example, two RD Session Hosts servers are part of this deployment.

Ensure that all RD Session Host servers are accessible on port **3389**. This can be done by opening the command line and running the command **telnet <IPAddressOfConnectionBroker> 3389** or use mstsc.exe to open an RDP connection to the RDP Connection Broker.

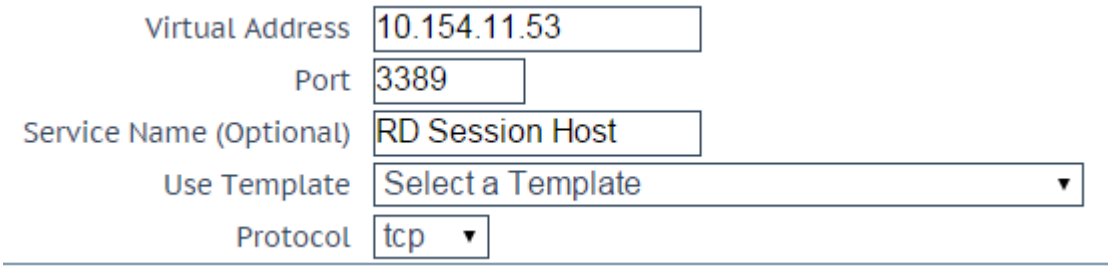
Load Balanced DNS Name	Load Balanced IP Address
rdshfarm.rdpdoc.net	10.154.11.53

Also, ensure you have an IP address and DNS available that are used to access the load balanced RD Session Host environment. In our example, the above information was used.

Implementation

Configure the LoadMaster settings by following the steps below in the LoadMaster WUI:

1. In the main menu, select **Virtual Services** and **Add New**.



2. Enter the relevant IP address in the **Virtual Address** text box.

   Note: In our example, the IP address is **10.154.11.53**

3. Enter **3389** as the **Port**.
4. Enter a recognizable **Service Name**, such as **RD Session Host**.
5. Click **Add this Virtual Service**.

Section	Option	Value	Comment
Basic Properties	Service Type	Remote Terminal	
Standard Options	Transparency	Disabled	
	Persistence Mode	Session Broker	The LoadMaster is able to redirect a user to an existing (disconnected) session based on the persistence token. If you performed a deployment without an RD Connection Broker (role-based deployment), the persistence token is the pre-populated username sent by the client. Also, the pre-populated username relies on users to always pre-populate the username field and is limited to a total of eight characters including the domain name.
	Persistence Timeout	1 Hour	
	Scheduling Method	least connection	To ensure that user sessions are equally spread over the RD Session Host servers, select the option Least Connection, or if you have configured a Weight on the Real Servers, set it to Weighted Least Connection.
	Idle Connection Timeout	660	
Real Servers	Real Server Check	Remote Terminal Protocol	

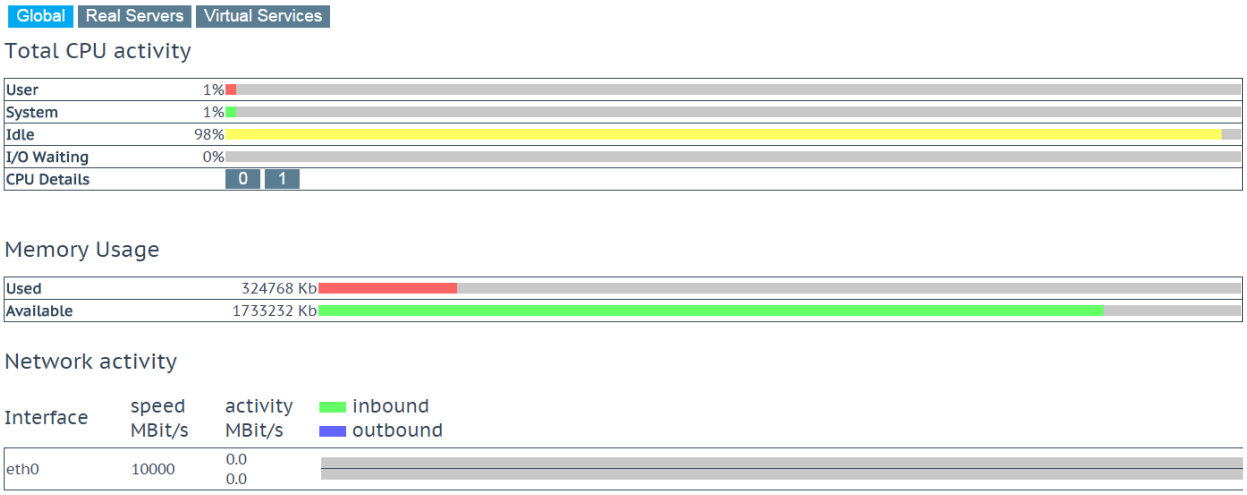
Section	Option	Value	Comment
	Method		
	Checked Port	3389	
	Forwarding method	Nat	

6. Enter the settings based on the recommended values above.

Testing

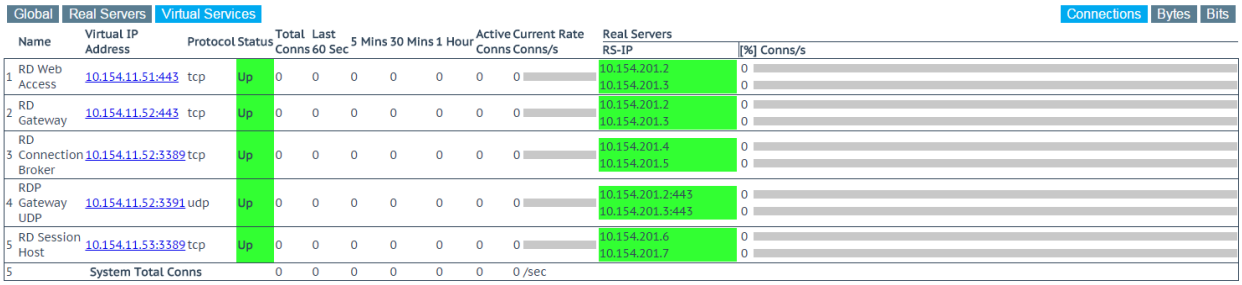
After following the implementation steps in the previous section, follow the steps below to test the load balanced RD Session Host environment:

1. Open an RDP connection to the RDS 2012 deployment to make sure the destination of your RDP session points to the DNS name configured earlier (which points to the IP address of the RD Session Host Virtual Service). In our example, it is **rsdhfarm.rdpdoc.net**.
2. In the main menu of the LoadMaster WUI, select **Statistics**.



3. Click the **Virtual Services** button.

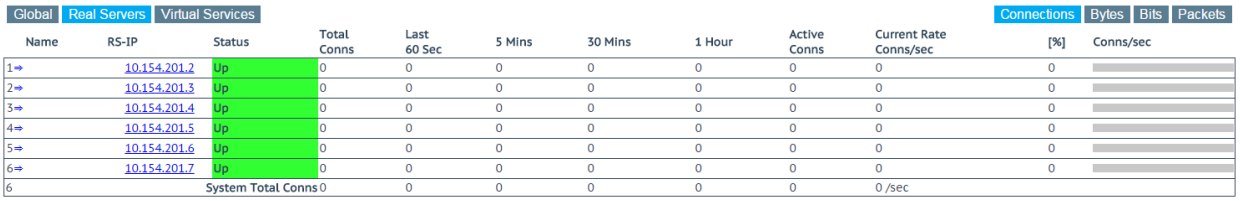
Note: This overview shows the active sessions, sessions over the last hour, in addition to how many requests each Real Server handled.



Global | Real Servers | Virtual Services — Connections | Bytes | Bits

	Name	Virtual IP Address	Protocol	Status	Total Conns	Last 60 Sec	5 Mins	30 Mins	1 Hour	Active Conns	Current Rate Conns/s	Real Servers RS-IP	[%] Conns/s
1	RD Web Access	10.154.11.51:443	tcp	Up	0	0	0	0	0	0	0	10.154.201.2 10.154.201.3	0 0
2	RD Gateway	10.154.11.52:443	tcp	Up	0	0	0	0	0	0	0	10.154.201.2 10.154.201.3	0 0
3	RD Connection Broker	10.154.11.52:3389	tcp	Up	0	0	0	0	0	0	0	10.154.201.4 10.154.201.5	0 0
4	RDP Gateway UDP	10.154.11.52:3391	udp	Up	0	0	0	0	0	0	0	10.154.201.2:443 10.154.201.3:443	0 0
5	RD Session Host	10.154.11.53:3389	tcp	Up	0	0	0	0	0	0	0	10.154.201.6 10.154.201.7	0 0
5	System Total Conns				0	0	0	0	0	0	0 /sec		

4. Open another web browser on a different client and perform steps 1 and 2 above.



Global | Real Servers | Virtual Services — Connections | Bytes | Bits | Packets

Name	RS-IP	Status	Total Conns	Last 60 Sec	5 Mins	30 Mins	1 Hour	Active Conns	Current Rate Conns/sec	[%]	Conns/sec
1⇒	10.154.201.2	Up	0	0	0	0	0	0	0	0	
2⇒	10.154.201.3	Up	0	0	0	0	0	0	0	0	
3⇒	10.154.201.4	Up	0	0	0	0	0	0	0	0	
4⇒	10.154.201.5	Up	0	0	0	0	0	0	0	0	
5⇒	10.154.201.6	Up	0	0	0	0	0	0	0	0	
6⇒	10.154.201.7	Up	0	0	0	0	0	0	0	0	
6	System Total Conns		0	0	0	0	0	0	0 /sec		

5. Refresh the LoadMaster statistics page. Notice that, based on the load balancing method we chose, load is spread over both RD Session Host servers.

3

Troubleshooting

Refer to the sections below for details on some common issues seen when load balancing the RDP workload.

Connections Rejected

Windows Server 2012 and 2012 R2 have security requirements on IIS. Therefore, when RDP traffic is reencrypted from the LoadMaster, the server thinks it is a “Man in the Middle” attack and rejects the connection. The following Microsoft article describes this behavior: https://support.microsoft.com/en-us/kb/973917

There are a few ways to work around this issue:

- Use the same SSL certificate on the LoadMaster and on the RD Gateway server.
- Configure the RD Gateway server to expect offload and accept connections on port 80 with no encryption. Configure the LoadMaster to offload (with no reencryption).
- Configure IIS as per the Microsoft article: https://support.microsoft.com/en-us/kb/973917 with the following changes:

- appcmd.exe set config "Default Web Site" -section:system.webServer/security/authentication/windowsAuthentication /enabled:"True" /commit:apphost
- appcmd.exe set config "Default Web Site" -section:system.webServer/security/authentication/windowsAuthentication /extendedProtection.tokenChecking:"Allow" /extendedProtection.flags:"Proxy" /commit:apphost
- appcmd.exe set config "Default Web Site" -section:system.webServer/security/authentication/windowsAuthentication /+"extendedProtection.[name='HTTP/rdgateway.contoso.com']" /commit:apphost

Load Not Balanced

There is a nine character limit in RDP sessions from Microsoft. Therefore, if an RDP session comes in using the domain first, the LoadMaster persists that client to a server without balancing the load. This behavior is as a result of the routing token character limitation and is not caused by the LoadMaster.

Refer to the following Microsoft article for instructions on how to specify custom routing tokens: IMsRdpClientAdvancedSettings::LoadBalanceInfo property

4

References

Some resources on Microsoft RDS 2012 (R2) are listed below:

What's New in Remote Desktop Services for Windows Server 2012 R2?

Remote Desktop Services – Upgrade and Migration Guidelines for Windows Server 2012 R2

Load Balancing Remote Desktop Services Web Access & Gateway with LoadMaster for Azure

Deploying and Configuring RD Web Access in Windows Server 2012

Deploying and Configuring RD Connection Broker High Availability in Windows Server 2012

RD Connection Broker Database Explained

Publishing RemoteApps in Windows Server 2012

Microsoft Remote Desktop Clients

A useful, related Progress Kemp document is listed below:

SSL Accelerated Services, Feature Description