Copyright Notices

Copyright © 2002-2016 KEMP Technologies, Inc.. All rights reserved.. KEMP Technologies and the KEMP Technologies logo are registered trademarks of KEMP Technologies, Inc..

KEMP Technologies, Inc. reserves all ownership rights for the LoadMaster product line including software and documentation. The use of the LoadMaster Exchange appliance is subject to the license agreement. Information in this guide may be modified at any time without prior notice.

Microsoft Windows is a registered trademarks of Microsoft Corporation in the United States and other countries. All other trademarks and service marks are the property of their respective owners.

Limitations: This document and all of its contents are provided as-is. KEMP Technologies has made efforts to ensure that the information presented herein are correct, but makes no warranty, express or implied, about the accuracy of this information. If any material errors or inaccuracies should occur in this document, KEMP Technologies will, if feasible, furnish appropriate correctional notices which Users will accept as the sole and exclusive remedy at law or in equity. Users of the information in this document acknowledge that KEMP Technologies cannot be held liable for any loss, injury or damage of any kind, present or prospective, including without limitation any direct, special, incidental or consequential damages (including without limitation lost profits and loss of damage to goodwill) whether suffered by recipient or third party or from any action or inaction whether or not negligent, in the compiling or in delivering or communicating or publishing this document.

Any Internet Protocol (IP) addresses, phone numbers or other data that may resemble actual contact information used in this document are not intended to be actual addresses, phone numbers or contact information. Any examples, command display output, network topology diagrams, and other figures included in this document are shown for illustrative purposes only. Any use of actual addressing or contact information in illustrative content is unintentional and coincidental.

Portions of this software are; copyright (c) 2004-2006 Frank Denis. All rights reserved; copyright (c) 2002 Michael Shalayeff. All rights reserved; copyright (c) 2003 Ryan McBride. All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer

2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

THIS SOFTWARE IS PROVIDED BY THE ABOVE COPYRIGHT HOLDERS "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE ABOVE COPYRIGHT HOLDERS OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

The views and conclusions contained in the software and documentation are those of the authors and should not be interpreted as representing official policies, either expressed or implied, of the above copyright holders.

Portions of the LoadMaster software are copyright (C) 1989, 1991 Free Software Foundation, Inc. -51 Franklin Street, Fifth Floor, Boston, MA 02110-1301, USA- and KEMP Technologies Inc. is in full compliance of the GNU license requirements, Version 2, June 1991. Everyone is permitted to copy and distribute verbatim copies of this license document, but changing it is not allowed.
Portions of this software are Copyright (C) 1988, Regents of the University of California. All rights reserved. Redistribution and use in source and binary forms are permitted provided that the above copyright notice and this paragraph are duplicated in all such forms and that any documentation, advertising materials, and other materials related to such distribution and use acknowledge that the software was developed by the University of California, Berkeley. The name of the University may not be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED "AS IS" AND WITHOUT ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, WITHOUT LIMITATION, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE.

Portions of this software are Copyright (C) 1998, Massachusetts Institute of Technology

Permission is hereby granted, free of charge, to any person obtaining a copy of this software and associated documentation files (the "Software"), to deal in the Software without restriction, including without limitation the rights to use, copy, modify, merge, publish, distribute, sublicense, and/or sell copies of the Software, and to permit persons to whom the Software is furnished to do so, subject to the following conditions:

The above copyright notice and this permission notice shall be included in all copies or substantial portions of the Software.

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.

Portions of this software are Copyright (C) 1995-2004, Jean-loup Gailly and Mark Adler

This software is provided 'as-is', without any express or implied warranty. In no event will the authors be held liable for any damages arising from the use of this software.

Permission is granted to anyone to use this software for any purpose, including commercial applications, and to alter it and redistribute it freely, subject to the following restrictions:

1. The origin of this software must not be misrepresented; you must not claim that you wrote the original software. If you use this software in a product, an acknowledgment in the product documentation would be appreciated but is not required.

2. Altered source versions must be plainly marked as such, and must not be misrepresented as being the original software.

3. This notice may not be removed or altered from any source distribution.

Portions of this software are Copyright (C) 2003, Internet Systems Consortium

Permission to use, copy, modify, and/or distribute this software for any purpose with or without fee is hereby granted, provided that the above copyright notice and this permission notice appear in all copies.

THE SOFTWARE IS PROVIDED "AS IS" AND THE AUTHOR DISCLAIMS ALL WARRANTIES WITH REGARD TO THIS SOFTWARE INCLUDING ALL IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS. IN NO EVENT SHALL THE AUTHOR BE LIABLE FOR ANY SPECIAL, DIRECT, INDIRECT, OR CONSEQUENTIAL DAMAGES OR ANY DAMAGES WHATSOEVER RESULTING FROM LOSS OF USE, DATA OR PROFITS, WHETHER IN AN ACTION OF CONTRACT, NEGLIGENCE OR OTHER TORTIOUS ACTION, ARISING OUT OF OR IN CONNECTION WITH THE USE OR PERFORMANCE OF THIS SOFTWARE.

Used, under license, U.S. Patent Nos. 6,473,802, 6,374,300, 8,392,563, 8,103,770, 7,831,712, 7,606,912, 7,346,695, 7,287,084 and 6,970,933.
Table of Contents

1 Introduction .................................................................................................................................................. 5
  1.1 Document Purpose ............................................................................................................................... 5
  1.2 Intended Audience .............................................................................................................................. 5

2 RDS Load Balancing Scenarios .................................................................................................................. 6
  2.1 Scenarios Explained ............................................................................................................................. 6
    2.1.1 Load Balancing Remote Desktop Web Access ............................................................................... 6
    2.1.2 Load Balancing Remote Desktop Gateway ................................................................................... 7
    2.1.3 Load Balancing Remote Desktop Connection Broker ................................................................. 8
    2.1.4 Load Balancing Remote Desktop Session Host ............................................................................... 8
  2.2 Deploying the Scenarios ......................................................................................................................... 9
    2.2.1 Prerequisites ................................................................................................................................... 9
    2.2.2 Implementing Remote Desktop Web Access Load Balancing ....................................................... 10
    2.2.3 Implementing Remote Desktop Gateway Load Balancing ............................................................ 15
    2.2.4 Implementing Remote Desktop Connection Broker Load Balancing ........................................... 27
    2.2.5 Implementing Remote Desktop Session Host Load Balancing ..................................................... 33

3 Troubleshooting ......................................................................................................................................... 38

References ...................................................................................................................................................... 39

Document History ......................................................................................................................................... 40
1 Introduction

Remote Desktop Services (RDS), which was 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. This evolved in RDP 8.1 with Windows Server 2012 R2 and Windows 8.1. Compared to previous releases, a lot has changed regarding both the administrative experience as well as the user experience.

1.1 Document Purpose

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

Section 2.1 discusses the various scenarios in which the LoadMaster can be used. Section 2.2 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.

1.2 Intended Audience

This document is intended to be read by anyone who is interested in finding out how to configure the LoadMaster to load balance RDS.
2 RDS Load Balancing Scenarios

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

2.1 Scenarios Explained

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

2.1.1 Load Balancing Remote Desktop Web Access

Microsoft Remote Desktop Web Access is used to publish Full Desktops as well as Remote Apps and make them available via a website, and a web feed.

Load balancing Remote Desktop Web Access (RD Web Access) is relatively straight forward. 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.
Once your RD Web Access server have 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 need to be added to the LoadMaster to start load balancing Web Access.

### 2.1.2 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 needs to be load balanced in the KEMP LoadMaster.

Once the RD Gateway role has been 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.
2.1.3 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 will make sure that users will be able to reconnect to an existing (disconnected) session. Since Windows Server 2012, end users connecting to the environment will always make an initial RDP connection to the RD Connection Broker. The RD Connection Broker will then reroute the user to the RD Session Host server with the least load (based on the load balancing mechanism within the RD Connection Broker) or reroute the user to an existing (disconnected) session.

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

![RD Connection Broker FQDNs](image)

Once the RD Connection Broker role has been 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.

2.1.4 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 needs to be load balanced in the LoadMaster. In this scenario, the RD Connection Broker role functionality to redirect to an existing (disconnected) session will still be in place, but the RD Connection Broker itself will not actively load balance sessions across RD Session Host servers.
Once the RD Session Host role has been 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.

### 2.2 Deploying the Scenarios

#### 2.2.1 Prerequisites

An SSL certificate is required to be installed on the LoadMaster for some of the services being load balanced.

Before we import the certificate make sure you have it available to the user who manages the LoadMaster. The certificate needs to match the hostname which is used to connect to the load balanced services of the LoadMaster and 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**.

   ![Certificate Configuration](image)

   **Figure 2-6: Import Certificate**

2. Click **Import Certificate**.
Remote Desktop Services

RDS Load Balancing Scenarios

Figure 2-7: Select the 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**.
8. Click **OK**.

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

Figure 2-8: Administrative Certificate

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**.

2.2.2 Implementing Remote Desktop Web Access Load Balancing

2.2.2.1 Prerequisites

As discussed in Section 2.1.1, implementing load balancing for RD Web Access can be compared with a regular web site running based on the HTTPS protocol (port 443).

Before configuring the KEMP 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.

<table>
<thead>
<tr>
<th>RD Web Access Server</th>
<th>IP Address</th>
</tr>
</thead>
<tbody>
<tr>
<td>RDP-RDGW01.rdpdoc.net</td>
<td>10.154.201.2</td>
</tr>
<tr>
<td>RDP-RDGW01.rdpdoc.net</td>
<td>10.154.201.3</td>
</tr>
</tbody>
</table>

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.

<table>
<thead>
<tr>
<th>Load Balanced DNS Name</th>
<th>Load Balanced IP Address</th>
</tr>
</thead>
<tbody>
<tr>
<td>rdpweb.rdpdoc.net</td>
<td>10.154.11.51</td>
</tr>
</tbody>
</table>

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

Ensure that a valid SSL certificate has been configured within the RDS deployment which is trusted by the endpoints that will be 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.
Figure 2-14: Manage certificates

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

2.2.2.2 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.

Figure 2-15: Add a Virtual Service
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.

<table>
<thead>
<tr>
<th>Section</th>
<th>Option</th>
<th>Value</th>
<th>Comment</th>
</tr>
</thead>
<tbody>
<tr>
<td>Standard Options</td>
<td>Transparency</td>
<td>Disabled</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Persistence Method</td>
<td>None</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Scheduling Method</td>
<td>least connection</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Idle Connection Timeout</td>
<td>660</td>
<td>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.</td>
</tr>
<tr>
<td>SSL Properties</td>
<td>SSL Acceleration</td>
<td>Enabled Reencrypt</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Supported Protocols</td>
<td>TLS1.0, TLS1.1, TLS1.2</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Cipher Set</td>
<td>Best Practices</td>
<td>For further information on cipher sets, please refer to the SSL Accelerated Services, Feature Description.</td>
</tr>
<tr>
<td>Advanced Properties</td>
<td>Content Switching</td>
<td>Disabled</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Add HTTP Headers</td>
<td>Legacy Operation (X-ClientSide)</td>
<td></td>
</tr>
<tr>
<td>Real Servers</td>
<td>Real Server Check Parameters</td>
<td>HTTPS Protocol</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Checked Port</td>
<td>443</td>
<td></td>
</tr>
<tr>
<td></td>
<td>URL</td>
<td>/rdweb</td>
<td></td>
</tr>
<tr>
<td></td>
<td>HTTP Method</td>
<td>HEAD</td>
<td></td>
</tr>
</tbody>
</table>

Table 1: Web Access Values

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.

2.2.2.3 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.

![Figure 2-16: Statistics screen](image)

4. Click the Real Servers button.

![Figure 2-17: Real Server statistics](image)

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.

![Figure 2-18: Statistics](image)

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.

### 2.2.3 Implementing Remote Desktop Gateway Load Balancing

#### 2.2.3.1 Prerequisites

As explained in Section 2.1.2, 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.
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.

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

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

Ensure that a valid SSL certificate has been configured within the RDS deployment which is trusted by the endpoints that will be 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.

### 2.2.3.2 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.

   **In our example, the IP address is** 10.154.11.52.

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

<table>
<thead>
<tr>
<th>Section</th>
<th>Option</th>
<th>Value</th>
<th>Comment</th>
</tr>
</thead>
<tbody>
<tr>
<td>Standard Options</td>
<td>Transparency</td>
<td>Disabled</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Persistence Mode</td>
<td>Source IP Address</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Persistence Timeout</td>
<td>6 Minutes</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Scheduling Method</td>
<td>least connection</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Idle Connection Timeout</td>
<td>660</td>
<td></td>
</tr>
<tr>
<td>SSL Properties</td>
<td>SSL Acceleration</td>
<td>Reencrypt</td>
<td>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.</td>
</tr>
<tr>
<td></td>
<td>SSL Acceleration</td>
<td>Reencrypt</td>
<td></td>
</tr>
<tr>
<td>Supported Protocols</td>
<td>TLS1.0</td>
<td>TLS1.1</td>
<td>TLS1.2</td>
</tr>
<tr>
<td>Cipher Set</td>
<td>Best Practices</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Advanced Properties</td>
<td>Content Switching</td>
<td>Disabled</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Add HTTP Headers</td>
<td>Legacy Operation(X-ClientSide)</td>
<td></td>
</tr>
<tr>
<td>Real Servers</td>
<td>Real Server Check Method</td>
<td>HTTPS Protocol</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Checked Port</td>
<td>443</td>
<td></td>
</tr>
<tr>
<td></td>
<td>URL</td>
<td>/rpc</td>
<td></td>
</tr>
<tr>
<td>HTTP Method</td>
<td>HEAD</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

6. Fill out the settings based on the recommended values above.

RDP version 8 and above contains new features that uses 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, we need to configure the RD Gateway to allow load balancing of UDP traffic. To do this, follow the steps below:

1. In the main menu of the LoadMaster WUI, select **Virtual Services > Add New**.
2. 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`.

3. Enter `3391` as the **Port**.

4. Select `udp` as the **Protocol**.

5. Click **Add this Virtual Service**.

<table>
<thead>
<tr>
<th>Section</th>
<th>Option</th>
<th>Value</th>
<th>Comment</th>
</tr>
</thead>
<tbody>
<tr>
<td>Standard Options</td>
<td>Force L7</td>
<td>Disabled</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Transparency</td>
<td>Enabled</td>
<td></td>
</tr>
<tr>
<td>Persistence Mode</td>
<td>Persistence Timeout</td>
<td>Source IP Address</td>
<td>6 Minutes</td>
</tr>
<tr>
<td>Scheduling Method</td>
<td>least connection</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

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 has been configured to an RD Gateway Server, selecting Weighted Least Connection here would also add the configured weight as a factor in calculating the schedule.

### Table 3: RDS Gateway UDP Virtual Service Values

<table>
<thead>
<tr>
<th>Real Servers</th>
<th>Real Server Check Method</th>
<th>Port</th>
<th>Forwarding Method</th>
<th>Direct return</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>443</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

6. Fill out the settings based on the recommended values above.

The UDP traffic for RDP version 8 is configured to use Direct Server Return (DSR). Therefore, we need to make some changes to the RD Gateway Servers in order 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 will create a new network adapter. To make it easier to identify, rename it, for example to KEMP 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. Please enter the name of the loopback adapter where <loopback> is mentioned. Please 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> weakhostend=enabled

2.2.3.3 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 Section 2.1.1.
   – Use the Remote App and Desktop Connections (RADC) as part of the Control Panel
   – Manually create a .RDP file.
Ensure to actually 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.

![Figure 2-34: Statistics screen](image1)

3. Click the Virtual Services button.

![Figure 2-35: Virtual Service statistics](image2)

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.

![Figure 2-36: Statistics](image3)

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:

1. Log in to the RD Gateway Server that holds the active test session.
2. Open Administrative Tools and then Remote Desktop Gateway Manager.
3. Expand your RD Gateway server and click Monitoring.
4. Confirm that your active session uses HTTP as the Transport, and not RPC-HTTP.

### 2.2.4 Implementing Remote Desktop Connection Broker Load Balancing

#### 2.2.4.1 Prerequisites

As discussed in Section 2.1.3, implementing load balancing for RD Connection Broker is performed by load balancing RDP traffic on port 3389. In this scenario we will load balance the initial sessions that users will perform on the RD Connection Broker.

Before configuring the KEMP 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.

<table>
<thead>
<tr>
<th>RD Web Access Server</th>
<th>IP Address</th>
</tr>
</thead>
<tbody>
<tr>
<td>RDP-RDCB01.rdpdoc.net</td>
<td>10.154.201.4</td>
</tr>
<tr>
<td>RDP-RDCB01.rdpdoc.net</td>
<td>10.154.201.5</td>
</tr>
</tbody>
</table>

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.

<table>
<thead>
<tr>
<th>Load Balanced DNS Name</th>
<th>Load Balanced IP Address</th>
</tr>
</thead>
<tbody>
<tr>
<td>rdsfarm.rdpdoc.net</td>
<td>10.154.11.52</td>
</tr>
</tbody>
</table>

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

The DNS name needs to 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 has been configured within the RDS deployment which is trusted by the endpoints that will be 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.

2.2.4.2 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.

   ![Add a Virtual Service](image)

   **Figure 2-45: Add a Virtual Service**

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

<table>
<thead>
<tr>
<th>Section</th>
<th>Option</th>
<th>Value</th>
<th>Comment</th>
</tr>
</thead>
<tbody>
<tr>
<td>Standard Options</td>
<td>Transparency</td>
<td>Disabled</td>
<td>In the Standard Options section, a Persistence Mode can be specified.</td>
</tr>
<tr>
<td></td>
<td>Persistence Mode</td>
<td>Terminal Service or Source IP Address</td>
<td>The RD Connection Broker role itself does not rely on persistence.</td>
</tr>
<tr>
<td></td>
<td>Persistence Timeout</td>
<td>6 minutes</td>
<td>This is because the RD Connection Broker servers will only handle the</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>initial RDP request, it does not contain any active sessions. Therefore,</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>the persistence mode can be left to the default option.</td>
</tr>
<tr>
<td></td>
<td>Scheduling Method</td>
<td>Round robin</td>
<td>Because the RD Connection Broker servers do not contain any active sessions the scheduling method does not really matter. Round Robin is the best suited option as this will ensure that the load is equally spread over the RD Connection Broker servers. Alternatively, choose Weighted Round Robin if the Real Servers have a non-default weight set.</td>
</tr>
<tr>
<td>Idle Connection Timeout</td>
<td></td>
<td>660</td>
<td></td>
</tr>
<tr>
<td>Real Servers</td>
<td>Real Server Check Method</td>
<td>Remote Terminal Protocol</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Checked Port</td>
<td>3389</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Forwarding method</td>
<td>Nat</td>
<td>Table 4: RDS Connection Broker Virtual Service Values</td>
</tr>
</tbody>
</table>

6. Fill out the settings based on the recommended values above.

2.2.4.3 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 Section 2.1.1.
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**.

![Figure 2-46: Statistics screen](image)

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

![Figure 2-47: Virtual Service statistics](image)

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.

![Figure 2-48: Statistics](image)

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.
2.2.5 Implementing Remote Desktop Session Host Load Balancing

2.2.5.1 Prerequisites

As discussed in Section 2.1.4, 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 will automatically get an RD Connection Broker as part of your deployment. This RD Connection Broker will automatically start load balancing sessions for the RD Session Host servers in your deployment. We’ll obviously want to avoid this to because it will result in double load balancing.

To disable RD Connection Broker Load balancing 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\User RD Connection Broker load balancing
```

Disabling the option 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.

```
P lease 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 KEMP LoadMaster, ensure to have the DNS names and IP addresses available for all Web Servers running the RD Session Host role.

![Deployment Servers](image)

**Figure 2-50: RD Web Access Server FQDNs**

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.

![PowerShell results](image)

**Figure 2-51: PowerShell results**

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

<table>
<thead>
<tr>
<th>RD Web Access Server</th>
<th>IP Address</th>
</tr>
</thead>
<tbody>
<tr>
<td>RDP-RDCB01.rdpdoc.net</td>
<td>10.154.201.6</td>
</tr>
<tr>
<td>RDP-RDCB01.rdpdoc.net</td>
<td>10.154.201.7</td>
</tr>
</tbody>
</table>

**Figure 2-52: IP Addresses**

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

### 2.2.5.2 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**.

   
<table>
<thead>
<tr>
<th>Virtual Address</th>
<th>Port</th>
<th>Service Name (Optional)</th>
<th>Use Template</th>
<th>Protocol</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.154.11.53</td>
<td>3389</td>
<td>RD Session Host</td>
<td>Select a Template</td>
<td>tcp</td>
</tr>
</tbody>
</table>

   **Figure 2-54: Add a Virtual Service**

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

   **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**.
Remote Desktop Services

RDS Load Balancing Scenarios

<table>
<thead>
<tr>
<th>Section</th>
<th>Option</th>
<th>Value</th>
<th>Comment</th>
</tr>
</thead>
<tbody>
<tr>
<td>Basic Properties</td>
<td>Service Type</td>
<td>Remote Terminal</td>
<td></td>
</tr>
<tr>
<td>Standard Options</td>
<td>Transparency</td>
<td>Disabled</td>
<td>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 will be 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 8 characters including the domain name.</td>
</tr>
<tr>
<td></td>
<td>Persistence Mode</td>
<td>Session Broker</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Persistence Timeout</td>
<td>6 minutes</td>
<td></td>
</tr>
<tr>
<td>Scheduling Method</td>
<td>Least connection</td>
<td></td>
<td>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.</td>
</tr>
<tr>
<td>Idle Connection Timeout</td>
<td>660</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Real Servers</td>
<td>Real Server Check Method</td>
<td>Remote Terminal Protocol</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Checked Port</td>
<td>3389</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Forwarding method</td>
<td>Nat</td>
<td></td>
</tr>
</tbody>
</table>

Table 5: RDS Session Host Virtual Service Values

6. Fill out the settings based on the recommended values above.

2.2.5.3 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.
Remote Desktop Services

RDS Load Balancing Scenarios

Figure 2-55: Statistics screen

3. Click the Virtual Services button.

Figure 2-56: Virtual Service statistics

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.

Figure 2-57: Statistics

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

Windows Server 2012 and 2012 R2 have security requirements on IIS. So when RDP traffic is reencrypted from the LoadMaster, the server thinks it’s a “Man in the Middle” attack and rejects the connection. The following Microsoft article describes this behaviour: 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.[name='HTTP/rdgateway.contoso.com']" /commit:apphost
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 KEMP LoadMaster for Azure](#)
- [Deploying and Configuring RD Gateway in Windows Server 2012](#)
- [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](#)
- [Distribution of Remote Apps and Desktops in Windows Server 2012](#)
- [Publishing RemoteApps in Windows Server 2012](#)
- [Microsoft Remote Desktop Clients](#)

A useful, related KEMP document is listed below:

- [SSL Accelerated Services, Feature Description](#)
  [www.kemptechnologies.com/documentation](http://www.kemptechnologies.com/documentation)
## Document History

<table>
<thead>
<tr>
<th>Date</th>
<th>Change</th>
<th>Reason for Change</th>
<th>Version</th>
<th>Resp.</th>
</tr>
</thead>
<tbody>
<tr>
<td>June 2014</td>
<td>Initial draft</td>
<td>First draft of document</td>
<td>1.0</td>
<td>LB</td>
</tr>
<tr>
<td>Nov 2014</td>
<td>Minor change</td>
<td>Defects resolved</td>
<td>1.1</td>
<td>LB</td>
</tr>
<tr>
<td>Oct 2015</td>
<td>Screenshot updates</td>
<td>LoadMaster WUI reskin</td>
<td>3.0</td>
<td>KG</td>
</tr>
<tr>
<td>Dec 2015</td>
<td>Release updates</td>
<td>Updated for 7.1-32</td>
<td>4.0</td>
<td>LB</td>
</tr>
<tr>
<td>Jan 2016</td>
<td>Minor change</td>
<td>Updated Copyright Notices</td>
<td>5.0</td>
<td>LB</td>
</tr>
<tr>
<td>Mar 2016</td>
<td>Release updates</td>
<td>Updated for 7.1-34</td>
<td>6.0</td>
<td>LB</td>
</tr>
<tr>
<td>May 2016</td>
<td>Minor change</td>
<td>Enhancements made</td>
<td>7.0</td>
<td>LB</td>
</tr>
</tbody>
</table>