Table of Contents

About this Guide .................................................................................................................................................. 4
Loadbalancer.org Appliances Supported ........................................................................................................... 4
Loadbalancer.org Software Versions Supported ................................................................................................. 4
Microsoft Windows Versions Supported .............................................................................................................. 4
Remote Desktop Services .................................................................................................................................. 5
  Introduction ...................................................................................................................................................... 5
  Role Services ................................................................................................................................................... 5
  Windows 2008 R2 RDS Deployment Overview ............................................................................................... 6
  Windows 2012 RDS Deployment Overview ...................................................................................................... 7
Load Balancing Remote Desktop Services ........................................................................................................ 9
  Basic Concepts .................................................................................................................................................. 9
  Load Balanced Ports & Services .......................................................................................................................... 9
  Persistence (Server Affinity) Requirements & Options ....................................................................................... 9
    Connection Broker Persistence ....................................................................................................................... 10
    Client Source IP Address Persistence ........................................................................................................... 10
    RDP Cookie Persistence .................................................................................................................................. 10
Remote Desktop Services – Load Balancing Scenarios ................................................................................... 11
  Scenario 1 - Load Balancing Stand alone Session Hosts .................................................................................... 11
  Scenario 2 - Load Balancing Connection Brokers with Session Hosts .............................................................. 12
  Scenario 3 - Load Balancing Connection Brokers with Virtualization Hosts ..................................................... 13
  Scenario 4 - Load Balancing Session Hosts when Deployed with Connection Broker ...................................... 14
  Scenario 5 - Load Balancing Gateways ........................................................................................................... 15
  Scenario 6 - Load Balancing Web Access Servers .......................................................................................... 16
Loadbalancer.org Appliance – the Basics ........................................................................................................... 17
  Initial Network Configuration ............................................................................................................................. 17
  Accessing the Web User Interface (WUI) ........................................................................................................... 18
  Clustered Pair Configuration .............................................................................................................................. 19
Load Balancing Session Hosts when Deployed without Connection Broker (Scenario 1) ............................ 20
  RDS Installation & Configuration ...................................................................................................................... 20
  Load Balancer Configuration ............................................................................................................................. 20
    Setting up the Virtual Service (VIP) ................................................................................................................. 20
    Setting up the Real Servers (RIPs) .................................................................................................................... 21
    Applying the new Layer 7 Settings ................................................................................................................... 21
  Testing & Verification ....................................................................................................................................... 21
Load Balancing Connection Brokers (Scenario’s 2 & 3) ................................................................................... 22
  RDS Installation & Configuration ...................................................................................................................... 22
  Load Balancer Configuration ............................................................................................................................. 22
    Setting up the Virtual Service (VIP) ................................................................................................................. 22
    Setting up the Real Servers (RIPs) .................................................................................................................... 23
    Applying the new Layer 7 Settings ................................................................................................................... 24
  Testing & Verification ....................................................................................................................................... 24
Load Balancing Session Hosts when Deployed with Connection Broker (Scenario 4) ............................. 25
  RDS Installation & Configuration ...................................................................................................................... 25
  Load Balancer Configuration ............................................................................................................................. 26
    Setting up the Virtual Service (VIP) ................................................................................................................. 26
    Setting up the Real Servers (RIPs) .................................................................................................................... 26
    Applying the new Layer 7 Settings ................................................................................................................... 27
  Testing & Verification ....................................................................................................................................... 27
Load Balancing Gateways (Scenario 5) ............................................................................................................ 28
  RDS Installation & Configuration ...................................................................................................................... 28
  Load Balancer Configuration ............................................................................................................................. 29
    Setting up the TCP Virtual Service (VIP) ......................................................................................................... 29
    Setting up the TCP Real Servers (RIPs) ........................................................................................................... 30
    Applying the new Layer 7 Settings ................................................................................................................... 30
About this Guide

This guide details the configuration of Loadbalancer.org appliances for deployment with Microsoft Remote Desktop Services (RDS). The guide focuses on Windows 2012 and later, although reference is made to 2008 R2 where appropriate.

The guide also details any required Remote Desktop Services configuration changes that are required to enable load balancing using Loadbalancer.org appliances.

For an introduction on setting up the appliance as well as more technical information, please also refer to our quick–start guide and full administration manual which are available at the following links:

**Version 7 Documentation**


**Version 8 Documentation**


Loadbalancer.org Appliances Supported

All our products can be used with Remote Desktop Services. The complete list of models is shown below:

<table>
<thead>
<tr>
<th>Discontinued Models</th>
<th>Current Models *</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enterprise R16</td>
<td>Enterprise R20</td>
</tr>
<tr>
<td>Enterprise VA R16</td>
<td>Enterprise MAX</td>
</tr>
<tr>
<td>Enterprise VA</td>
<td>Enterprise 10G</td>
</tr>
<tr>
<td></td>
<td>Enterprise R320</td>
</tr>
<tr>
<td></td>
<td>Enterprise VA R20</td>
</tr>
<tr>
<td></td>
<td>Enterprise VA MAX</td>
</tr>
<tr>
<td></td>
<td>Enterprise AWS **</td>
</tr>
<tr>
<td></td>
<td>Enterprise AZURE **</td>
</tr>
</tbody>
</table>

* For full specifications of these models please refer to: [http://www.loadbalancer.org/products](http://www.loadbalancer.org/products)

** Some features may not be supported, please check with Loadbalancer.org support

Loadbalancer.org Software Versions Supported

•  v7.6 and later

Microsoft Windows Versions Supported

•  Windows 2008 R2 and later
Remote Desktop Services

Introduction

Remote Desktop Services accelerates and extends desktop and application deployments to any device, improving remote worker efficiency, while helping to keep critical intellectual property secure and simplify regulatory compliance. Remote Desktop Services enables virtual desktop infrastructure (VDI), session-based desktops, and applications, allowing users to work anywhere.

Role Services

The following role services can be deployed as part of the RDS role.

<table>
<thead>
<tr>
<th>Role Service</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>RD Virtualization Host</td>
<td>Remote Desktop Virtualization Host integrates with Hyper-V to deploy pooled or personal virtual desktop collections within your organization.</td>
</tr>
<tr>
<td>RD Session Host</td>
<td>Remote Desktop Session Host enables a server to host RemoteApp programs or session-based desktops. Users can connect to RD Session Host servers in a session collection to run programs, save files, and use resources on those servers.</td>
</tr>
<tr>
<td>RD Connection Broker</td>
<td>Allows users to reconnect to their existing virtual desktops, RemoteApp programs, and session-based desktops. Enables you to evenly distribute the load among RD Session Host servers in a session collection or pooled virtual desktops in a pooled virtual desktop collection. Provides access to virtual desktops in a virtual desktop collection.</td>
</tr>
<tr>
<td>RD Web Access</td>
<td>Remote Desktop Web Access enables users to access RemoteApp and Desktop Connection through the Start menu on a computer that is running Windows 8, Windows 7, or through a web browser. RemoteApp and Desktop Connection provides a customized view of RemoteApp programs and session-based desktops in a session collection, and RemoteApp programs and virtual desktops in a virtual desktop collection.</td>
</tr>
<tr>
<td>RD Licensing</td>
<td>Remote Desktop Licensing manages the licenses required to connect to a Remote Desktop Session Host server or a virtual desktop. You can use RD Licensing to install, issue, and track the availability of licenses.</td>
</tr>
<tr>
<td>RD Gateway</td>
<td>Remote Desktop Gateway enables authorized users to connect to virtual desktops, RemoteApp programs, and session-based desktops on an internal corporate network from any Internet-connected device.</td>
</tr>
</tbody>
</table>
Windows 2008 R2 RDS Deployment Overview

Installation of RDS under Windows 2008 R2 uses the traditional role/service concept. The RDS infrastructure must be built by manually installing the required services on the various servers to build the desired infrastructure.

The screenshot below shows the initial service selection screen for installing RDS under Windows 2008 R2.
Windows 2012 RDS Deployment Overview

Windows 2012 provides two installation types, the first is the **Role-based or feature-based** installation where roles and services are installed on individual servers as per Windows 2008 R2 and secondly **Remote Desktop Services Installation** which is a centrally based installation which enables all role services to be installed on multiple servers from one place which is a substantial improvement on 2008 R2.

The **Remote Desktop Services Installation type** supports 2 deployment types – the **Standard deployment** option allows RDS to be deployed across multiple servers, the **Quick Start** option deploys all services to one server.
The Standard deployment type supports two deployment scenarios, these are Virtual machine-based desktop deployment (aka. "Virtual Desktop Infrastructure" in Win2008 R2) and Session-based desktop deployment (i.e. the traditional 'terminal server' type deployments):

A typical completed deployment is shown below:

Methods Used in this Guide

In this guide both the Role-based or feature-based and Remote Desktop Services Installation types are used depending on the particular load balancing scenario. Please refer to pages 11 to 16 for details of the various scenario's.
Load Balancing Remote Desktop Services

Basic Concepts

The load balancer is deployed in front of the various RDS servers to provide load balancing and fail-over functionality. Clients then connect to a Virtual Service (VIP) on the load balancer rather than connecting directly to a one of the RDS servers. These connections are then load balanced between the associated RDS servers to distribute the load according to the load balancing algorithm selected.

Using a Loadbalancer.org clustered pair with multiple Microsoft RDS servers enables the following key benefits:

- **High-Availability** – Servers are continually health checked by the load balancer and are automatically removed from the load balanced pool if the health check fails

- **Performance** – Adding additional servers distributes the load and improves performance

- **Maintainability** – Servers can easily be removed from the pool in a controlled manner to allow maintenance tasks such as applying software updates to be carried out

Load Balanced Ports & Services

The following table shows the RDS ports and service that are load balanced:

<table>
<thead>
<tr>
<th>Protocol</th>
<th>Port</th>
<th>Purpose / Service</th>
</tr>
</thead>
<tbody>
<tr>
<td>TCP/HTTPS</td>
<td>443</td>
<td>HTTPS (RD Gateway, RD Web Access)</td>
</tr>
<tr>
<td>TCP/UDP/RDP</td>
<td>3389</td>
<td>RDP (UDP support was added in RDP v8.0)</td>
</tr>
<tr>
<td>UDP</td>
<td>3391</td>
<td>RDP (RD Gateway)</td>
</tr>
</tbody>
</table>

Persistence (Server Affinity) Requirements & Options

Persistence means consistently sending a particular client to the same back-end server during a particular session. This is critical for some role services and not relevant to others. The following table summarises the requirements:

<table>
<thead>
<tr>
<th>Service</th>
<th>Persistence Required?</th>
<th>Comments</th>
<th>Persistence Methods</th>
</tr>
</thead>
<tbody>
<tr>
<td>Virtualization Hosts</td>
<td>Yes</td>
<td>Required to enable users to reconnect to their desktops</td>
<td>Connection Broker</td>
</tr>
<tr>
<td>Session Hosts</td>
<td>Yes</td>
<td>Required to enable users to reconnect to their session</td>
<td>Connection Broker or Client source IP address</td>
</tr>
<tr>
<td>Connection Brokers</td>
<td>No</td>
<td>Data is stored in an SQL DB, brokers only relay the request</td>
<td>-</td>
</tr>
<tr>
<td>Gateways</td>
<td>Yes</td>
<td>Both SSL connections must go to the same Gateway server</td>
<td>Client source IP address</td>
</tr>
<tr>
<td>Web Access Servers</td>
<td>Yes</td>
<td>Uses IIS with authentication which is to a specific server</td>
<td>Client source IP address</td>
</tr>
</tbody>
</table>
**Connection Broker Persistence**

Remote Desktop Connection Broker provides the following functionality:

- Allows users to reconnect to their existing virtual desktops, RemoteApp programs, and session-based desktops
- Enables you to evenly distribute the load among RD Session Host servers in a session collection or pooled virtual desktops in a pooled virtual desktop collection
- Provides access to virtual desktops in a virtual desktop collection

All user sessions are stored as records in a central SQL database. The database is updated and queried by the RDS servers whenever users log on, log off, or disconnect their sessions.

The load balancer is able to interact with Connection Broker by enabling **Routing Token Redirection Mode** on the RDS servers. This mode allows the reconnection of disconnected sessions by utilizing a routing token to enable the load balancer to re-connect the client to the correct Session Host.

*N.B. For more information on how this works please refer to the following Microsoft URLs:

a) **Redirection Modes**

b) **Session Directory and Load Balancing Using Terminal Server**

(Written for Win2003, but the redirection concepts on p25 to p27 also apply to Win2008 & Win2012)

**Client Source IP Address Persistence**

This method is appropriate when each client's actual source IP addresses can be seen by the load balancer. This will typically be the case within a LAN but in some situations – e.g. a remote office connecting via some kind of NAT device, all clients would appear to come from the same address and therefore load may not be evenly distributed between the RDS servers.

**RDP Cookie Persistence**

This persistence method utilises the cookie sent from the client in the Connection Request PDU. The cookie is created when the username is entered at the first client login prompt when using mstsc.exe. However, in certain scenarios depending on client version as well as the specific client & server settings, the RDP cookie (mstshash) is not consistently sent so cannot be relied on. Please refer to our blog post for more information:
http://blog.loadbalancer.org/microsoft-drops-support-for-mstshash-Cookies/

**Update (October 2015)** – with the latest versions of the various Windows clients, this problem appears to have been resolved.

*N.B. From v7.6.3, when RDP cookie persistence is selected, the load balancer will attempt to use RDP cookie persistence, but if a cookie is not found, source IP persistence will be used instead. This may be appropriate in some circumstances, although in this guide this persistence method is not used.*
Remote Desktop Services – Load Balancing Scenarios

Scenario 1 - Load Balancing Stand alone Session Hosts

**Client Connection Process:**

1. Client initiates session request to the VIP on the load balancer
2. If the client has connected previously, and the persistence (stick) table entry has not timed out, the load balancer forwards the request to the same session host, if the client has not connected previously or the stick-table entry has expired, the request is load balanced to one of the session hosts according to the load balancing algorithm selected
3. The client continues the session to the selected session host via the load balancer (assuming a Layer 7 configuration as used in this guide)

**Notes:**

- In this scenario connection broker is not used
- Session persistence from client to session host is based on client source IP address
- Clients connect using the Microsoft RDP client (mstsc.exe) or equivalent
- Management is possible via local PowerShell commands, or by using RDMS on a Windows 2008 or other remote host
- Layer 7 SNAT mode is used for the VIP in this guide. It’s also possible to use Layer 4 DR or NAT mode depending on your infrastructure and requirements (see pages 36 and 37)

*N.B. For more details on using Session Host without Connection Broker, please refer to the following Microsoft link: [http://support.microsoft.com/kb/2833839](http://support.microsoft.com/kb/2833839)*

See page 20 for load balancer configuration steps and RDS configuration notes related to this scenario.
Scenario 2 - Load Balancing Connection Brokers with Session Hosts

Client Connection Process:

1. Client initiates session request to the VIP on the load balancer
2. The load balancer forwards the request to one of the load balanced connection brokers
3. The connection broker checks the SQL database to determine if the user has an existing session, if yes the IP address for that server is selected, if no then the RDS built in load balancing mechanism selects a host / IP address where to start a new session
4. The connection broker returns this IP address back to the client via the load balancer (assuming a Layer 7 configuration as used in this guide)
5. The client connects directly to the session host specified

Notes:

- In this scenario the initial connection is to the connection brokers (via the load balancer) and not the session hosts, this is because in Win2012 the connection brokers also act as redirectors
- Session persistence from client to connection broker is not required
- Clients connect using RemoteAPP via RD Web Access or modified .rdp files and not mstsc.exe. Please refer to the following link for more information: http://microsoftplatform.blogspot.co.uk/2012/04/rd-connection-broker-ha-and-rdp.html
- Layer 7 SNAT mode is used for the VIP in this guide. It’s also possible to use Layer 4 DR or NAT mode depending on your infrastructure and requirements (see pages 36 and 37)

See page 22 for load balancer configuration steps and RDS configuration notes related to this scenario.
Scenario 3 - Load Balancing Connection Brokers with Virtualization Hosts

Client Connection Process:

1. Client initiates session request to the VIP on the load balancer
2. The load balancer forwards the request to one of the load balanced connection brokers
3. The connection broker checks the SQL database to determine if the user has an existing session, if yes the IP address for that server is selected, if no then the RDS built in load balancing mechanism selects a host / IP address where to start a new session
4. The connection broker returns this IP address back to the client via the load balancer (assuming a Layer 7 configuration as used in this guide)
5. The client connects directly to the virtualization host specified

Notes:

- In this scenario the initial connection is to the connection brokers (via the load balancer) and not the virtualization hosts, this is because in Win2012 the connection brokers also act as redirectors
- Session persistence from client to connection broker is not required
- Clients connect using RemoteAPP via RD Web Access or modified .rdp files and not mstsc.exe. Please refer to the following link for more information:
  http://microsoftplatform.blogspot.co.uk/2012/04/rd-connection-broker-ha-and-rdp.html
- Layer 7 SNAT mode is used for the VIP in this guide. It's also possible to use Layer 4 DR or NAT mode depending on your infrastructure and requirements (see pages 36 and 37)

See page 22 for load balancer configuration steps and RDS configuration notes related to this scenario.
Scenario 4 - Load Balancing Session Hosts when Deployed with Connection Broker

Client Connection Process:

1. Client initiates session request to the VIP on the load balancer
2. The load balancer forwards the request to one of the load balanced session hosts
3. The session host checks with the active connection broker if the user has an existing session, if yes the IP address for that server is encoded in a **routing token**
4. The **routing token** is returned via the load balancer to the client, the client then reconnects via the load balancer to the session host specified in the **routing token**

* N.B. For more information on routing tokens and their format please refer to the following URL:

Notes:

- In this scenario the initial connection is to the session hosts which perform the client redirection
- The session hosts must be configured in **Routing Token Redirection Mode** (see page 25)
- Session persistence from client to session host is based on routing token
- Layer 7 SNAT mode must be used for this configuration to enable the routing tokens to be read
- Clients connect using the Microsoft RDP client (mstsc.exe) or equivalent

See page 25 for load balancer configuration steps and RDS configuration notes related to this scenario.
Scenario 5 - Load Balancing Gateways

Client Connection Process:

1. Client initiates session request to the VIP on the load balancer
2. The load balancer forwards the request to one of the load balanced gateway servers
3. The selected gateway forwards the connection to the load balanced connection broker VIP where the connection is load balanced to one of the connection brokers, and in turn onto the relevant session host. This process is the same as the load balanced connection broker scenario on pages 12 & 13

Notes:

- Clients connect using RemoteAPP via RD Web Access or modified .rdp files
- Session persistence from client to gateway is based on client source IP address
- 2 VIPs are used, one Layer 7 SNAT mode VIP is used for the HTTPS connection and one layer 4 DR mode VIP is used for UDP. It’s also possible to use Layer 4 NAT mode rather than DR mode depending on your infrastructure and requirements (see pages 36 and 37)

See page 28 for load balancer configuration steps and RDS configuration notes related to this scenario.
Scenario 6 - Load Balancing Web Access Servers

Client Connection Process:

1. Client initiates session request to the VIP on the load balancer
2. The load balancer forwards the request to one of the load balanced web access servers
3. The client continues the session to the selected web access server via the load balancer (assuming a Layer 7 configuration as used in this guide)

Notes:

- Web access servers use IIS so it's effectively the same as load balancing standard Microsoft Web Servers
- Session persistence from client to web access server is based on client source IP address
- The Web Access servers have a built-in HTTP --> HTTPS redirect, so the VIP also listens on port 80 to enable this to function correctly
- Layer 7 SNAT mode is used for the example in this guide. It's also possible to use Layer 4 DR or NAT modes depending on your infrastructure and requirements (see pages 36 and 37)

See page 33 for load balancer configuration steps and RDS configuration notes related to this scenario.
Loadbalancer.org Appliance – the Basics

Initial Network Configuration
The IP address, subnet mask, default gateway and DNS settings can be configured in several ways as detailed below:

Method 1 - Using the Network Setup Wizard at the console
After boot up, follow the instructions on the console to configure the IP address, subnet mask, default gateway and DNS settings.

Method 2 - Using the WUI:
Using a browser, connect to the WUI on the default IP address/port: http://192.168.2.21:9080
To set the IP address & subnet mask, use: Local Configuration > Network Interface Configuration
To set the default gateway, use: Local Configuration > Routing
To configure DNS settings, use: Local Configuration > Hostname & DNS

Method 3 - Using Linux commands:
At the console, set the initial IP address using the following command:

```
ip addr add <IP address>/<mask> dev eth0
e.g.
ip addr add 192.168.2.10/24 dev eth0
```

At the console, set the initial default gateway using the following command:

```
route add default gw <IP address> <interface>
e.g.
rout add default gw 192.168.2.254 eth0
```

At the console, set the DNS server using the following command:

```
echo nameserver <IP address> >> /etc/resolv.conf
e.g.
echo nameserver 192.168.2.250 >> /etc/resolv.conf
```

N.B. If method 3 is used, you must also configure these settings using the WUI, otherwise the settings will be lost after a reboot
Accessing the Web User Interface (WUI)

The WUI can be accessed from a browser at:  http://192.168.2.21:9080/lbadmin

* Note the port number → 9080

(replace 192.168.2.21 with the IP address of your load balancer if it's been changed from the default)

Username: loadbalancer
Password: loadbalancer

Once you have entered the logon credentials the Loadbalancer.org Web User Interface will be displayed as shown below:
The screen shot below shows the v7.6 WUI once logged in:

Clustered Pair Configuration

Loadbalancer.org recommend that load balancer appliances are deployed in pairs for high availability. In this guide a single unit is deployed first, adding a secondary slave unit is covered in section 5 of the Appendix.
Load Balancing Session Hosts when Deployed without Connection Broker (Scenario 1)

Please refer to page 11 for a deployment diagram and notes on how the load balancer interacts with RDS.

RDS Installation & Configuration

- Use the *Role-based or feature-based* installation type to install the Session Host service on multiple servers
- Session management on Windows 2008 hosts is via *Remote Desktop Services Manager*
- In this scenario, session management on Windows 2012 hosts is not possible using graphical tools, only Powershell. However, *Remote Desktop Services Manager* on Windows 2008 / Windows 7 (Remote Server Administration Tools for Windows 7) can also be used to manage Window 2012 hosts

Load Balancer Configuration

Setting up the Virtual Service (VIP)

- Go to *Cluster Configuration > Layer 7 – Virtual Services* and click [Add a New Virtual Service]
- Enter the following details:
  - Enter an appropriate name (Label) for the Virtual Service, e.g. *SH-Cluster*
  - Set the *Virtual Service IP address* field to the required IP address, e.g. *192.168.2.100*
  - Set the *Virtual Service Ports* field to *3389*
  - Set the *Layer 7 Protocol* to *TCP Mode*
  - Click *Update*
  - Now click [Modify] next to the newly created Virtual Service
  - Ensure *Persistence Mode* is set to *Source IP*
  - Set *Persistence Timeout* to an appropriate value, e.g. *120* (i.e. 2 hours)
  - Enable (check) the *Timeout* checkbox and set both *Client & Real Server Timeout* to *2h* (i.e. 2 hours)
  - Click *Update*
Setting up the Real Servers (RIPs)

- Go to Cluster Configuration > Layer 7 – Real Servers and click [Add a New Real Server] next to the newly created Virtual Service

- Enter the following details:

  - Enter an appropriate name (Label) for the first RDS server, e.g. SH1
  - Change the Real Server IP Address field to the required IP address, e.g. 192.168.2.200
  - Set the Real Server Port field to 3389
  - Click Update

- Now repeat for your remaining Session Host server(s)

Applying the new Layer 7 Settings

- Once the configuration is complete, use the Reload HAProxy button at the top of the screen to commit the changes

Testing & Verification

The load balanced Session Host servers should now be accessible using the VIP address or corresponding DNS host name if one has been created. Connect to this address from the Microsoft RDP client (mstsc.exe) or equivalent.
Load Balancing Connection Brokers (Scenario’s 2 & 3)

Please refer to pages 12 & 13 for a deployment diagram and notes on how the load balancer interacts with RDS.

RDS Installation & Configuration

- Use the *Remote Desktop Services* installation type to install Connection Broker, Web Access and Session Host / Virtualization Host role services to the relevant RDS servers.
- The initial client connection is load balanced across the Connection Brokers by the appliance, client to session host / virtualization host sessions are load balanced using the built-in load balancing mechanism. Health checking is periodically performed by the connection brokers. The health check interval and other related settings can be changed using the following registry path on each connection broker server:

```
HKLM/SYSTEM/CurrentControlSet/Services/Tssdis /Parameters
```

Please refer to the following Microsoft URL for more details on these settings:


Load Balancer Configuration

**Setting up the Virtual Service (VIP)**

- Go to *Cluster Configuration > Layer 7 – Virtual Services* and click [Add a New Virtual Service]
- Enter the following details:
• Enter an appropriate name (Label) for the Virtual Service, e.g. **CB-Cluster**
• Set the **Virtual Service IP address** field to the required IP address, e.g. **192.168.2.110**
• Set the **Virtual Service Ports** field to **3389**
• Set the **Layer 7 Protocol** to **TCP Mode**
• Click **Update**
• Now click **[Modify]** next to the newly created Virtual Service
• Set **Persistence Mode** to **None**
• Click **Update**

**Setting up the Real Servers (RIPs)**

• Go to **Cluster Configuration > Layer 7 – Real Servers** and click **[Add a New Real Server]** next to the newly created Virtual Service

• Enter the following details:

  • Enter an appropriate name (Label) for the first RDS server, e.g. **CB1**
  • Change the **Real Server IP Address** field to the required IP address, e.g. **192.168.2.210**
  • Set the **Real Server Port** field to **3389**
  • Click **Update**
  • Now repeat for your remaining Connection Broker server(s)
Applying the new Layer 7 Settings

- Once the configuration is complete, use the Reload HAProxy button at the top of the screen to commit the changes

Testing & Verification

The load balanced Connection Broker servers should now be accessible via the DNS address. Use Web Access/RemoteAPP or a manually modified .rdp file to verify that published applications are available.

Ensure there is a valid DNS entry for the HA connection broker defined in the deployment settings. In this example it should be rdscb.robtest.com pointing to 192.168.2.110.
Load Balancing Session Hosts when Deployed with Connection Broker (Scenario 4)

Please refer to page 14 for a deployment diagram and notes on how the load balancer interacts with RDS.

**RDS Installation & Configuration**

- Use the *Remote Desktop Services* installation type to install Connection Broker, Web Access and Session Host Host role services to the relevant RDS servers
- Enable Routing Token Redirection Mode and disable the built in load balancing mechanism on each Session Host:
  - Using either a Group Policy Object that applies to all RDS servers or by configuring each server individually using local group policy, disable ‘Use IP Address Redirection’ & ‘Use RD Connection Broker load balancing’. Both settings can be accessed here:

<table>
<thead>
<tr>
<th>Computer Configuration</th>
<th>Administrative Templates</th>
<th>Windows Components</th>
<th>Remote Desktop Services</th>
<th>Remote Desktop Session Host</th>
<th>RD Connection Broker</th>
</tr>
</thead>
<tbody>
<tr>
<td>Join RD Connection Broker</td>
<td>Not configured</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Configure RD Connection Broker farm name</td>
<td>Not configured</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Use IP Address Redirection</td>
<td>Disabled</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Configure RD Connection Broker server name</td>
<td>Not configured</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Use RD Connection Broker load balancing</td>
<td>Disabled</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

  - The active connection broker can be set by selecting *Tasks* next to DEPLOYMENT OVERVIEW, then selecting ‘Set Active RD Connection Broker server’; then selecting the required server from the drop-down as shown below:

  ![Set Active RD Connection Broker Server](image)

  N.B. Please refer to section 4 in the Appendix for configuring Windows 2008 R2 for Routing Token Redirection Mode
Load Balancer Configuration

Setting up the Virtual Service (VIP)

- Go to Cluster Configuration > Layer 7 – Virtual Services and click [Add a New Virtual Service]
- Enter the following details:

  - Enter an appropriate name (Label) for the Virtual Service, e.g. **SH-Cluster**
  - Set the Virtual Service IP address field to the required IP address, e.g. **192.168.2.100**
  - Set the Virtual Service Ports field to **3389**
  - Set the Layer 7 Protocol to **TCP Mode**
  - Click Update
  - Now click [Modify] next to the newly created Virtual Service
  - Ensure Persistence Mode is set to **MS Session Broker**
  - Enable (check) the Timeout checkbox and set both Client & Real Server Timeout to **2h** (i.e. 2 hours)
  - Click Update

Setting up the Real Servers (RIPs)

- Go to Cluster Configuration > Layer 7 – Real Servers and click [Add a New Real Server] next to the newly created Virtual Service
- Enter the following details:
• Enter an appropriate name (Label) for the first RDS server, e.g. **SH1**
• Change the *Real Server IP Address* field to the required IP address, e.g. **192.168.2.200**
• Set the *Real Server Port* field to **3389**
• Click **Update**
• Now repeat for your remaining Session Host server(s)

**Applying the new Layer 7 Settings**

• Once the configuration is complete, use the **Reload HAProxy** button at the top of the screen to commit the changes

**Testing & Verification**

The load balanced Session Host servers should now be accessible using the VIP address or corresponding DSN host name if one has been created. Connect to this address from the Microsoft RDP client (mstsc.exe) or equivalent.
Load Balancing Gateways (Scenario 5)

Please refer to page 15 for a deployment diagram and notes on how the load balancer interacts with RDS.

RDS Installation & Configuration

- Use the Remote Desktop Services installation type to install Connection Broker, Web Access and Session Host / Virtualization Host role services to the relevant RDS servers.
- Right click the RD Gateway icon in the RDS Overview and add the Gateway role service to the relevant RDS servers.
- Ensure that the HA settings are configured correctly. These can be configured within the Deployment Properties:

  ![Configure the deployment](image)

  The DNS round robin setting is used by the Gateway servers to connect to the load balanced connection brokers. Create a DNS record with the same name that points to the load balanced Connection Broker VIP.

  - Ensure that the Gateway server setting is configured correctly. These can be configured within the Deployment Properties:

    ![Configure the deployment](image)

    Create a DNS record with the same name that points to the load balanced Gateway VIP.
• Ensure that the Remote Authorisation Policy policies permits connections to the session host servers and the DNS round robin HA name as shown below:

Now refer to section 2 in the Appendix to ensure that each gateway server is able to receive packets destined for the VIP address and that the servers do not respond to ARP requests for this IP address. This is known as *Solving the ARP problem.*

### Load Balancer Configuration

Two VIPs are required – one for the TCP/HTTPS component on port 443, the second is the for the UDP component on port 3391. Both VIPs are configured on the same IP address.

**Setting up the TCP Virtual Service (VIP)**

• Go to *Cluster Configuration > Layer 7 – Virtual Services* and click [Add a New Virtual Service]

• Enter the following details:

Enter an appropriate name (Label) for the Virtual Service, e.g. **GW-Cluster-TCP**

Set the Virtual Service IP address field to the required IP address, e.g. **192.168.2.120**

Set the Virtual Service Ports field to **443**

Set the Layer 7 Protocol to **TCP Mode**

Click **Update**

Now click [Modify] next to the newly created Virtual Service
• Ensure Persistence Mode is set to **Source IP**
• Set the Persistence Timeout to **120** (i.e. 2 hours)
• Enable (check) the Timeout checkbox and set both Client & Real Server Timeout to **2h** (i.e. 2 hours)
• Click **Update**

### Setting up the TCP Real Servers (RIPs)

• Go to *Cluster Configuration > Layer 7 – Real Servers* and click [Add a New Real Server] next to the newly created Virtual Service

• Enter the following details:

  ![Real Server Configuration](image)

  • Enter an appropriate name (Label) for the first gateway server, e.g. **GW1**
  • Change the Real Server IP Address field to the required IP address, e.g. **192.168.2.220**
  • Set the Real Server Port field to **443**
  • Click **Update**
  • Now repeat for your remaining Gateway server(s)

### Applying the new Layer 7 Settings

• Once the configuration is complete, use the **Reload HAProxy** button at the top of the screen to commit the changes

### Setting up the UDP Virtual Service (VIP)

• Go to *Cluster Configuration > Layer 4 – Virtual Services* and click [Add a New Virtual Service]

• Enter the following details:
• Enter an appropriate name (Label) for the Virtual Service, e.g. **GW-Cluster-UDP**
• Set the Virtual Service IP address field to the required IP address, e.g. **192.168.2.120**
• Set the Virtual Service Ports field to **3391**
• Set the Protocol to **UDP**
• Set the forwarding Method to **Direct Routing**
• Click **Update**
• Now click [Modify] next to the newly created Virtual Service
• Ensure the Persistence check-box is left unchecked
• Click **Update**

**Setting up the UDP Real Servers (RIPs)**

• Go to Cluster Configuration > Layer 4 – Real Servers and click [Add a New Real Server] next to the newly created Virtual Service

• Enter the following details:
  • Enter an appropriate name (Label) for the first gateway server, e.g. **GW1**
  • Change the Real Server IP Address field to the required IP address, e.g. **192.168.2.220**
  • Leave other values at the default values
• Click Update
• Now repeat for your remaining Gateway server(s)

Testing & Verification

The load balanced gateway servers should now be accessible via the DNS address. Use Web Access/RemoteAPP or a manually modified .rdp file to verify that published applications are available via the gateway.

Ensure there is a valid DNS entry for the HA connection broker defined in the deployment settings. In this example it should be the load balanced broker address: rdscb.robtest.com pointing to 192.168.2.110.

Ensure there is a valid DNS entry for the RD gateway server defined in the deployment settings. In this example it should be the load balanced gateway address: rd-gateway.robtest.com pointing to 192.168.2.120.
Load Balancing Web Access Servers (Scenario 6)

Please refer to page 16 for a deployment diagram and notes on how the load balancer interacts with RDS.

RDS Installation & Configuration

- Use the Remote Desktop Services installation type to install Connection Broker, Web Access and Session Host / Virtualization Host role services to the relevant RDS servers

Load Balancer Configuration

Setting up the Virtual Service (VIP)

- Go to Cluster Configuration > Layer 7 – Virtual Services and click [Add a New Virtual Service]
- Enter the following details:
  - Enter an appropriate name (Label) for the Virtual Service, e.g. **WA-Cluster**
  - Set the Virtual Service IP address field to the required IP address, e.g. **192.168.2.130**
  - Set the Virtual Service Ports field to **80,443**
  - Set the Layer 7 Protocol to **TCP Mode**
  - Click **Update**
  - Now click [Modify] next to the newly created Virtual Service
  - Ensure Persistence Mode is set to **Source IP**
  - Set Persistence Timeout to an appropriate value, e.g. **120** (i.e. 2 hours)
  - Enable (check) the Timeout checkbox and set both Client & Real Server Timeout to **2h** (i.e. 2 hours)
  - Click **Update**
Setting up the Real Servers (RIPs)

- Go to Cluster Configuration > Layer 7 – Real Servers and click [Add a New Real Server] next to the newly created Virtual Service

- Enter the following details:

  ![Real Server Details]

  - Enter an appropriate name (Label) for the first TS / RDS, e.g. WA1
  - Change the Real Server IP Address field to the required IP address, e.g. 192.168.2.230
  - Leave the Real Server Port field blank
  - Click Update
  - Now repeat for your remaining Web Access server(s)

Applying the new Layer 7 Settings

- Once the configuration is complete, use the Reload HAProxy button at the top of the screen to commit the changes

Testing & Verification

The load balanced Web Access servers should now be accessible using the VIP address or corresponding DNS entry if one has been created. Connect to this address from your browser.

In the case of the settings used here, the following URL would be used for RD Web Access:

https://192.168.2.130/RDweb
Technical Support
For more details or assistance with your deployment please don’t hesitate to contact the support team:
support@loadbalancer.org

Conclusion
Loadbalancer.org appliances provide a very cost effective and flexible solution for highly available load balanced Remote Desktop Services environments.
Appendix

1 - Supported Load Balancer Deployment Methods

The load balancer can be deployed in one of 3 fundamental ways: Layer 4 DR mode, Layer 4 NAT mode or Layer 7 SNAT mode. These are described below.

Layer 4 DR Mode (aka Direct Server Return)

One-arm Direct Routing (DR) mode is a very high performance solution that requires little change to your existing infrastructure.

- Direct Routing mode works by changing the destination MAC address of the incoming packet to match the selected Real Server on the fly which is very fast
- When the packet reaches the Real Server it expects it to own the Virtual Services IP address (VIP). This means that you need to ensure that the Real Server (and the load balanced application) respond to both the Real Servers own IP address and the VIP
- The Real Server should not respond to ARP requests for the VIP. Only the load balancer should do this. Configuring the Real Servers in this way is referred to as Solving the ARP Problem. please refer to chapter 6 in the administration manual for more information
- On average, DR mode is 8 times quicker than NAT for HTTP, 50 times quicker for Terminal Services and much, much faster for streaming media or FTP
- The load balancer must have an Interface in the same subnet as the Real Servers to ensure layer 2 connectivity required for DR mode to work
- The VIP can be brought up on the same subnet as the Real Servers, or on a different subnet provided that the load balancer has an interface in that subnet
- Port translation is not possible in DR mode i.e. having a different RIP port than the VIP port
- DR mode is transparent, i.e. the Real Server will see the source IP address of the client

N.B. Layer 4 DR mode is used for the Gateway UDP requirement in this guide
Layer 4 NAT Mode

Sometimes it’s not possible to use DR mode. The two most common reasons being: if the application cannot bind to the RIP & VIP at the same time; or if the host operating system cannot be modified to handle the ARP problem. The second choice is Network Address Translation (NAT) mode. This is also a high performance solution but it requires the implementation of a two arm infrastructure with an internal and external subnet to carry out the translation (the same way a firewall works).

- The load balancer translates all requests from the external Virtual Service to the internal Real Servers
- Normally eth0 is used for the internal network and eth1 is used for the external network although this is not mandatory. If the Real Servers require Internet access, Autonat should be enabled using the WUI option: Cluster Configuration > Layer 4 – Advanced Configuration, the external interface should be selected
- NAT mode can be deployed in the following ways:
  2-arm (using 2 Interfaces), 2 subnets (as shown above) - One interface on the load balancer is connected to subnet1 and the second interface and Real Servers are connected to subnet2. The VIP is brought up in subnet1. The default gateway on the Real Servers is set to be an IP address in subnet2 on the load balancer. Clients can be located in subnet1 or any remote subnet provided they can route to the VIP
  2-arm (using 1 Interface), 2 subnets - same as above except that a single interface on the load balancer is allocated 2 IP addresses, one in each subnet
  1-arm (using 1 Interface), 1 subnet - Here, the VIP is brought up in the same subnet as the Real Servers. For clients located in remote networks the default gateway on the Real Servers must be set to be an IP address on the load balancer. For clients located on the same subnet, return traffic would normally be sent directly to the client bypassing the load balancer which would break NAT mode. To address this, the routing table on the Real Servers must be modified to force return traffic to go via the load balancer - for more details on ‘One-Arm NAT Mode’ please refer to chapter 6 in the administration manual
- If you want Real Servers to be accessible on their own IP address for non-load balanced services, e.g. SMTP or RDP, you will need to setup individual SNAT and DNAT firewall script rules for each Real Server or add additional VIPs for this - please refer to chapter 6 in the administration manual
- NAT mode is transparent, i.e. the Real Server will see the source IP address of the client
- Port translation is possible in NAT mode, i.e. VIP:80 → RIP8080 is possible
Layer 7 SNAT Mode

Layer 7 SNAT Mode is used in the application layer. Inbound requests are terminated on the load balancer, and HAProxy generates a new request to the chosen real server. As a result, Layer 7 is a slower technique than DR or NAT mode at Layer 4. Layer 7 is chosen when the network topology prohibits the use of layer 4 methods.

Single-arm and two-arm configurations are supported as shown below. In both cases return traffic passes via the load balancer. Since layer 7 works as a proxy, there is no need to set the appliance as the gateway.

Layer 7 SNAT Mode has the advantage of a one arm configuration and does not require any changes to the application servers. However, since the load balancer is acting as a full proxy it doesn’t have the same raw throughput as the layer 4 methods.

The network diagram for the Layer 7 HAProxy SNAT mode is very similar to the Direct Routing example except that no re-configuration of the Real Servers is required. The load balancer proxies the application traffic to the servers so that the source of all traffic becomes the load balancer.

- SNAT is a full proxy and therefore load balanced Real Servers do not need to be changed in any way
- Because SNAT is a full proxy any server in the cluster can be on any accessible subnet including across the Internet or WAN
- SNAT is not transparent by default, i.e. the Real Servers will not see the source IP address of the client, they will see the load balancers IP address. If required, this can be solved by either enabling TProxy on the load balancer, or for HTTP, using X-forwarded-For headers. Please refer to chapter 6 in the administration manual for more details.
- SNAT mode can be deployed using either a 1-arm or 2-arm configuration

This mode has the advantage of a one arm configuration and does not require any changes to the application servers. However, since the load balancer is acting as a full proxy it doesn’t have the same raw throughput as the layer 4 methods.

The network diagram for the Layer 7 HAProxy SNAT mode is very similar to the Direct Routing example except that no re-configuration of the Real Servers is required. The load balancer proxies the application traffic to the servers so that the source of all traffic becomes the load balancer.
2 - Solving the ARP Problem - Windows 2012

This process enables each server to be able to receive traffic destined for the VIP. It also also ensures that each server does not respond to ARP requests for the VIP address – only the load balancer should do this.

Step 1: Install the Microsoft Loopback Adapter

1. Click Start, then type `hdwwiz` and press <ENTER> to start the Hardware Installation Wizard
2. When the Wizard has started, click Next
3. Select Install the hardware that I manually select from a list (Advanced), click Next
4. Select Network adapters, click Next
5. Select Microsoft & Microsoft KM-Test Loopback Adapter, click Next

![Add Hardware]

6. Click Next to start the installation, when complete click Finish

Step 2: Configure the Loopback Adapter

1. Right click the Start/Windows button and select Network Connections
2. Click Change adapter settings
3. Right-click the new Loopback Adapter and select Properties
4. Un-check all items except **Internet Protocol Version 4 (TCP/IPv4)** as shown below

5. Select **Internet Protocol Version (TCP/IPv4)**, click **Properties** and configure the IP address to be the same as the Virtual Service (VIP) with a subnet mask of 255.255.255.255, e.g. 192.168.2.220 / 255.255.255.255 as shown below

6. Click **OK** on TCP/IP Properties, then click **Close** on Ethernet Properties to save and apply the new settings

7. Now repeat the above process on the other Gateway server(s)
Step 3: Configure the strong / weak host behaviour

To do this the following netsh commands must be run on each server:

```
netsh interface ipv4 set interface "net" weakhostreceive=enabled
netsh interface ipv4 set interface "loopback" weakhostreceive=enabled
netsh interface ipv4 set interface "loopback" weakhostsend=enabled
```

N.B. The names for the NICs are case sensitive, so make sure that the name used for the interface and the name used in the commands match exactly.

For these commands to work, the LAN connection NIC must be renamed "net" and the loopback NIC must be named "loopback" as shown below:

![Network Connections](image)

If you prefer to leave your current NIC names, then the commands above must be modified accordingly. For example, if your network adapters are named “LAN” and “LOOPBACK”, the commands required would be:

```
netsh interface ipv4 set interface "LAN" weakhostreceive=enabled
netsh interface ipv4 set interface "LOOPBACK" weakhostreceive=enabled
netsh interface ipv4 set interface "LOOPBACK" weakhostsend=enabled
```

1. Start Powershell, then run the 3 netsh commands as shown below:

![PowerShell Output](image)

2. Now repeat on the other Gateway server(s)

N.B. Solving the ARP problem for Windows 2008 R2 servers is very similar. For full details, please refer to the administration manual.
3 - Server Feedback Agent

The load balancer can dynamically modify the weight (amount of traffic) of each server by gathering data from a custom agent. Once installed and running, the agent listens on TCP port 3333. When the load balancer connects to this port, the agent responds with the idle stats as an integer value in the range 0–100. The figure returned can be related to CPU utilization, RAM usage or a combination of both. This can be configured using the XML configuration file located in the agents installation folder (by default this is located in C:\ProgramData\LoadBalancer.org\LoadBalancer).

This functionality enables intelligent load balancing based on the real time resource usage statistics of each RDS server. This is especially useful for session hosts where running client programs can easily saturate the servers resources.

For more information please also refer to the following blog article:

http://blog.loadbalancer.org/open-source-windows-service-for-reporting-server-load-back-to-haproxy-load-balancer-feedback-agent/

Windows Agent Download

The latest Windows feedback agent can be downloaded from:
http://downloads.loadbalancer.org/agent/loadbalanceragent.msi

To install the agent, run loadbalanceragent.msi on each RDS server.

Click Next
Select the installation folder and click **Next**

Click **Next** to start the installation

*N.B. .NET Framework v3.5 is required by the agent and .NET Framework v4.0 is required by the Monitor*

*N.B. The agent should be installed on each RDS server*
Starting the Agent

Once the installation has completed, you'll need to start the service on the RDS servers. The service is controlled by the Feedback Agent Monitor program that is also installed along with the Agent. The monitor can be accessed on the Windows server using: All Programs > Loadbalancer.org > Monitor. It's also possible to start the service using the services snap-in – the service is called 'Loadbalancer CPU monitor'.

- To start the service, click **Start**
- To stop the service, click **Stop**

Configuration

To Configure Virtual Services to use the feedback agent, follow the steps below:

- Go to Cluster Configuration > Layer 4 - Virtual Services or Layer 7 - Virtual Services
- Click **Modify** next to the Virtual Service
  
  ![Feedback Agent Monitor](image)

- Change the Feedback Method to **Agent**
- Click **Update**
- For layer 7 VIPs, restart HAProxy using the WUI option: Maintenance > Restart Services
4 - Configuring Windows 2008 R2 for Routing Token Redirection Mode

Install Connection Broker on the server designated to hold the Connection Broker role. Then on each RDS to be included in the cluster / Farm:

- Open Remote Desktop Host Session Configuration
- Right-click ‘Member of farm in RD Connection Broker’ and select Properties
- Click Change Settings
- Select Farm Member, enter the DNS name of the server running the Connection Broker role service and the name of the farm (all servers within the same farm require the same name to be specified) and click OK
- Leave Participate in Connection Broker Load-Balancing un-checked and select Use token redirection from the drop down as shown below:

5 - Clustered Pair Configuration – Adding a Slave Unit

If you initially configured just the master unit and now need to add a slave - our recommended procedure, please refer to the relevant document referenced below for more details:

**Version 7**

Please refer to Chapter 8 – Appliance Clustering for HA in the v7 Administration Manual.

**Version 8**

Please refer to Chapter 9 – Appliance Clustering for HA in the v8 Administration Manual.

Don’t hesitate to contact our support team if you need further assistance: support@loadbalancer.org
### 6 - Company Contact Information

<table>
<thead>
<tr>
<th>Website</th>
<th>URL: <a href="http://www.loadbalancer.org">www.loadbalancer.org</a></th>
</tr>
</thead>
</table>
| **North America (US)** | Loadbalancer.org, Inc.  
270 Presidential Drive  
Wilmington,  
DE 19807  
USA  
Tel: +1 888.867.9504 (24x7)  
Fax: +1 302.213.0122  
Email (sales): sales@loadbalancer.org  
Email (support): support@loadbalancer.org |
| **North America (Canada)** | Loadbalancer.org Ltd  
300–422 Richards Street  
Vancouver, BC  
V6B 2Z4  
Canada  
Tel: +1 855.681.6017 (24x7)  
Fax: +1 302.213.0122  
Email (sales): sales@loadbalancer.org  
Email (support): support@loadbalancer.org |
| **Europe (UK)** | Loadbalancer.org Ltd.  
Portsmouth Technopole  
Kingston Crescent  
Portsmouth  
PO2 8FA  
England, UK  
Tel: +44 (0)330 3801064 (24x7)  
Fax: +44 (0)870 4327672  
Email (sales): sales@loadbalancer.org  
Email (support): support@loadbalancer.org |
| **Europe (Germany)** | Loadbalancer.org GmbH  
Alt Pempelfort 2  
40211 Düsseldorf  
Germany  
Tel: +49 (0)30 920 383 6494  
Fax: +49 (0)30 920 383 6495  
Email (sales): vertrieb@loadbalancer.org  
Email (support): support@loadbalancer.org |