# Table of Contents

1. About this Guide ................................................................................................................. 4  
2. Loadbalancer.org Appliances Supported .............................................................................. 4  
3. Loadbalancer.org Software Versions Supported .................................................................... 4  
4. Microsoft Windows Versions Supported ............................................................................... 4  
5. Remote Desktop Services ...................................................................................................... 5  
   - Introduction ......................................................................................................................... 5  
   - Role Services ....................................................................................................................... 5  
   - Windows 2008 R2 RDS Deployment Overview .................................................................. 6  
   - Windows 2012 RDS Deployment Overview ....................................................................... 7  
6. 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  
7. Remote Desktop Services – Load Balancing Scenarios ....................................................... 12  
   - Scenario 1 - Load Balancing Stand alone Session Hosts .................................................... 12  
   - Scenario 2 - Load Balancing Connection Brokers with Session Hosts ............................. 13  
   - Scenario 3 - Load Balancing Connection Brokers with Virtualization Hosts .................. 14  
   - Scenario 4 - Load Balancing Session Hosts when Deployed with Connection Broker .... 15  
   - Scenario 5 - Load Balancing Gateways .......................................................................... 16  
   - Scenario 6 - Load Balancing Web Access Servers ............................................................ 17  
8. Loadbalancer.org Appliance – the Basics .......................................................................... 18  
   - Virtual Appliance Download & Deployment .................................................................... 18  
   - Initial Network Configuration ......................................................................................... 18  
   - Accessing the Web User Interface (WebUI) ..................................................................... 19  
   - HA Clustered Pair Configuration .................................................................................... 20  
9. Load Balancing Session Hosts Deployed without Connection Broker (Scenario 1) ........... 21  
   - RDS Installation & Configuration .................................................................................... 21  
   - Appliance Configuration .................................................................................................... 21  
   - Setting up the Virtual Service (VIP) .................................................................................. 21  
   - Setting up the Real Servers (RIPs) .................................................................................... 22  
   - Applying the new Layer 7 Settings .................................................................................... 22  
   - Testing & Verification ....................................................................................................... 22  
10. Load Balancing Connection Brokers (Scenario’s 2 & 3) ...................................................... 23  
    - RDS Installation & Configuration .................................................................................... 23  
    - Appliance Configuration .................................................................................................. 23  
    - Setting up the Virtual Service (VIP) ................................................................................ 23  
    - Setting up the Real Servers (RIPs) .................................................................................. 24  
    - Applying the new Layer 7 Settings .................................................................................. 24  
    - Testing & Verification ..................................................................................................... 25  
11. Load Balancing Session Hosts when Deployed with Connection Broker (Scenario 4) .... 25
1. About this Guide
This guide details the steps required to configure a load balanced Microsoft Remote Desktop Services (RDS) environment utilizing Loadbalancer.org appliances. It covers the configuration of the load balancers and also any Microsoft Remote Desktop Services configuration changes that are required to enable load balancing. The guide focuses on Windows 2012 and later, although reference is made to 2008 R2 where appropriate.
For more information about initial appliance deployment, network configuration and using the Web User Interface (WebUI), please also refer to the relevant Administration Manual:


2. 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>Enterprise R320</td>
<td>Enterprise Ultra</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/hardware](http://www.loadbalancer.org/products/hardware)
** Some features may not be supported, please check with Loadbalancer.org support

3. Loadbalancer.org Software Versions Supported

- V7.6.4 and later

4. Microsoft Windows Versions Supported

- Windows 2008 R2 and later
5. 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>
Remote Desktop Services

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.

![Select Role Services Screen](image-url)
**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 12 onward for details of
the various scenarios.

6. Load Balancing Remote Desktop Services

Note:
It’s highly recommended that you have a working RDS environment first before implementing
the load balancer.

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 summarizes
the requirements:

<table>
<thead>
<tr>
<th>Service</th>
<th>Persistence Required?</th>
<th>Comments</th>
<th>Load Balancer 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, client source IP address or RDP cookie (the specific</td>
</tr>
</tbody>
</table>
### Load Balancing Remote Desktop Services

<table>
<thead>
<tr>
<th>Method Supported Depends on Deployment Architecture</th>
<th>Connection Brokers</th>
<th>No</th>
<th>Data is stored in an SQL DB, brokers only relay the request</th>
<th>Persistence is not required since the load balancer only handles the initial connection and not the active RDP session</th>
</tr>
</thead>
<tbody>
<tr>
<td>Gateways</td>
<td>Yes</td>
<td></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></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 reconnect the client to the correct Session Host.

### Note:

For more information on how this works please refer to the following Microsoft URLs:

- [Redirection Modes](https://docs.microsoft.com/en-us/terminalservices/rd-deployment-guide/redirection-modes)

Note that b) was 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 method utilizes the cookie sent from the client in the Connection Request PDU. This cookie is created when the username is entered at the first client login prompt (mstsc.exe). If the username is not entered here, the cookie is not created.

The cookie only supports up to 9 characters, so this method may have limited use, especially in cases where users login using the domain\username format. In this case, if the domain name was 9 characters in length, the RDP cookie would be the same for all users, resulting in all sessions being sent to the same
session host. If users login using the UPN format (User Principle Name), i.e. `username@domain`, it’s more likely to be unique.

**Note:**

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 as a fallback.

**Note:**

In certain scenarios depending on client version as well as the specific client & server settings, the RDP cookie (mstshash) is not consistently sent. Please also refer to our blog post on this topic: [http://www.loadbalancer.org/blog/microsoft-drops-support-for-mstshash-cookies](http://www.loadbalancer.org/blog/microsoft-drops-support-for-mstshash-cookies).

**Update (October 2015)** – with the latest versions of Windows Servers & RDP Client, this problem appears to have been resolved.
7. 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 that was used for the previous session, 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
- In this scenario, session persistence can be based on client source IP address or the RDP cookie (mstshash) sent from the client in the Connection Request PDU
- 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 35 and 36)

Note:
For more details on using Session Host without Connection Broker, please refer to the following Microsoft link: http://support.microsoft.com/kb/2833839

Note:
See page 21 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 because it handles the initial request and not active RDP sessions
• 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 35 and 36)

Note:
See page 23 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 35 and 36)

Note:
See page 23 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**

**Note:**
For detailed information on routing tokens and their format please refer to [this document](#).

**Notes:**

- In this scenario the initial connection is to the session hosts which perform the client redirection
- One of the connection brokers must be configured as active (see page 25), active/active mode is only supported when used as part of a RD Gateway deployment (see pages 16)
- 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

**Note:**
See page 25 for load balancer configuration steps and RDS configuration notes.
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 connection broker, and in turn onto the relevant session host

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 part and one layer 4 DR mode VIP is used for the UDP part. It’s also possible to use Layer 4 NAT mode rather than DR mode depending on your infrastructure and requirements (see pages 35 and 36)
- There are 2 HTTPS channels, and if they can be established, 2 additional UDP channels per session. The 2 HTTPS channels need to be handled by the same gateway as do the 2 UDP channels, but the HTTPS and UDP channels can be handled by different gateways. For more information please refer to this link
- The RD Gateway deployment can also be configured to use connection brokers that are configured in HA mode. In this case, an additional VIP is required on the load balancer to load balance between the brokers. The DNS round robin name defined in the HA section of the deployment properties (see page 27) must resolve to this address.

Note:

See page 27 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 35 and 36)

Note:
See page 32 for load balancer configuration steps and RDS configuration notes related to this scenario.
8. Loadbalancer.org Appliance – the Basics

VIRTUAL APPLIANCE DOWNLOAD & DEPLOYMENT

A fully featured, fully supported 30 day trial is available if you are conducting a PoC (Proof of Concept) deployment. The VA is currently available for VMware, Virtual Box, Hyper-V, KVM and XEN and has been optimized for each Hypervisor. By default, the VA is allocated 1 CPU, 2GB of RAM and has an 8GB virtual disk. The Virtual Appliance can be downloaded [here](#).

**Note:**
The same download is used for the licensed product, the only difference is that a license key file (supplied by our sales team when the product is purchased) must be applied using the appliance's WebUI.

**Note:**
Please refer to the Administration Manual and the ReadMe.txt text file included in the VA download for more detailed information on deploying the VA using various Hypervisors.

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 WebUI**

Using a browser, connect to the WebUI on the default IP address/port: [http://192.168.2.21:9080](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
```

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

```
route add default gw <IP address> <interface>
```

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

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

**Note:**
If method 3 is used, you must also configure these settings using the WebUI, otherwise the settings will be lost after a reboot.
ACCESSING THE WEB USER INTERFACE (WEBUI)

The WebUI can be accessed via HTTP at the following URL: http://192.168.2.21:9080/lbadmin
* Note the port number → 9080

The WebUI can be accessed via HTTPS at the following URL: https://192.168.2.21:9443/lbadmin
* Note the port number → 9443

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

Login using the following credentials:

- **Username**: loadbalancer
- **Password**: loadbalancer

**Note:**
To change the password, use the WebUI menu option: Maintenance > Passwords.

Once logged in, the WebUI will be displayed as shown on the following page:
Loadbalancer.org Appliance – the Basics

HA 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 on page 45.
9. Load Balancing Session Hosts Deployed without Connection Broker (Scenario 1)

Please refer to page 12 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

APPLIANCE CONFIGURATION

SETTING UP THE VIRTUAL SERVICE (VIP)

1. Using the WebUI, navigate to: *Cluster Configuration > Layer 7 – Virtual Services* and click *Add a New Virtual Service*
2. Enter the following details:
   - **Label**: SH-Cluster
   - **Virtual Service IP Address**: 192.168.2.100
   - **Virtual Service Ports**: 3389
   - **Layer 7 Protocol**: TCP Mode
3. Enter an appropriate name (Label) for the Virtual Service, e.g. SH-Cluster
4. Set the **Virtual Service IP address** field to the required IP address, e.g. 192.168.2.100
5. Set the **Virtual Service Ports** field to 3389
6. Set the **Layer 7 Protocol** to **TCP Mode**
7. Click **Update**
8. Now click **Modify** next to the newly created Virtual Service
9. Configure the required **Persistence Mode**:
   - If you want to use the client source IP address to maintain client to server persistence, ensure **Persistence Mode** is set to **Source IP**
   - If you want to use RDP cookies to maintain client to server persistence, ensure **Persistence Mode** is set to **RDP Client Cookie**
10. Set **Persistence Timeout** to an appropriate value, e.g. 120 (i.e. 2 hours)
11. Enable (check) the **Timeout** checkbox and set both **Client Timeout & Real Server Timeout** to a suitable value, e.g. **2hr**

**Note:**
If persistence is set to RDP cookies, both timeout values are automatically set to 12h.

12. Click **Update**

**SETTING UP THE REAL SERVERS (RIPS)**

1. Using the WebUI, navigate to: **Cluster Configuration > Layer 7 – Real Servers** and click **Add a New Real Server** next to the newly created Virtual Service
2. Enter the following details:

   ![Real Server Configuration](image)

3. Enter an appropriate name (Label) for the first RDS server, e.g. **SH1**
4. Change the **Real Server IP Address** field to the required IP address, e.g. **192.168.2.200**
5. Set the **Real Server Port** field to **3389**
6. Click **Update**
7. Now repeat for your remaining Session Host server(s)

**APPLYING THE NEW LAYER 7 SETTINGS**

1. Once the configuration is complete, use the **Reload HAProy** 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.
10. Load Balancing Connection Brokers (Scenario's 2 & 3)

Please refer to pages 13 & 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/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:

- Ensure there is a valid DNS entry for the HA connection broker defined in the deployment settings. e.g. configure a DNS entry for rdscb.robstest.com pointing to the VIP address

APPLIANCE CONFIGURATION

SETTING UP THE VIRTUAL SERVICE (VIP)

1. Using the WebUI, navigate to: Cluster Configuration > Layer 7 – Virtual Services and click Add a New Virtual Service
2. Enter the following details:
3. Enter an appropriate name (Label) for the Virtual Service, e.g. **CB-Cluster**
4. Set the Virtual Service IP address field to the required IP address, e.g. **192.168.2.110**
5. Set the Virtual Service Ports field to **3389**
6. Set the Layer 7 Protocol to **TCP Mode**
7. Click **Update**
8. Now click **Modify** next to the newly created Virtual Service
9. Set Persistence Mode to **None**
10. Click **Update**

**SETTING UP THE REAL SERVERS (RIPS)**

1. Using the WebUI, navigate to: **Cluster Configuration > Layer 7 – Real Servers** and click **Add a New Real Server** next to the newly created Virtual Service
2. Enter the following details:

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

**APPLYING THE NEW LAYER 7 SETTINGS**

1. 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. As mentioned, 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.

11. Load Balancing Session Hosts when Deployed with Connection Broker (Scenario 4)
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 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:
  
  Computer Configuration | Administrative Templates | Windows Components | Remote Desktop Services | Remote Desktop Session Host | RD Connection Broker

<table>
<thead>
<tr>
<th>Setting</th>
<th>State</th>
</tr>
</thead>
<tbody>
<tr>
<td>Join RD Connection Broker</td>
<td>Not configured</td>
</tr>
<tr>
<td>Configure RD Connection Broker farm name</td>
<td>Not configured</td>
</tr>
<tr>
<td>Use IP Address Redirection</td>
<td>Disabled</td>
</tr>
<tr>
<td>Configure RD Connection Broker server name</td>
<td>Not configured</td>
</tr>
<tr>
<td>Use RD Connection Broker load balancing</td>
<td>Disabled</td>
</tr>
</tbody>
</table>

Note:
Please refer to section 4 in the Appendix on page 45 for configuring Windows 2008 R2 for Routing Token Redirection Mode.

- 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:
APPLIANCE CONFIGURATION

SETTING UP THE VIRTUAL SERVICE (VIP)

1. Using the WebUI, navigate to: Cluster Configuration > Layer 7 – Virtual Services and click **Add a New Virtual Service**
2. 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)

1. Using the WebUI, navigate to: Cluster Configuration > Layer 7 – Real Servers and click **Add a New Real Server** next to the newly created Virtual Service
2. Enter the following details:
Load Balancing Session Hosts when Deployed with Connection Broker (Scenario 4)

3. Enter an appropriate name (Label) for the first RDS server, e.g. **SH1**
4. Change the **Real Server IP Address** field to the required IP address, e.g. **192.168.2.200**
5. Set the **Real Server Port** field to **3389**
6. Click **Update**
7. Now repeat for your remaining Session Host server(s)

**APPLYING THE NEW LAYER 7 SETTINGS**

1. 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.

**12. Load Balancing Gateways (Scenario 5)**

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
- Right click the RD Gateway icon in the RDS Overview and add the Gateway role service to the relevant RDS servers
- Ensure that the Gateway server setting is configured correctly. These can be configured within the Deployment Properties:
• Create a DNS record with the same name (rd-gateway.robstest.com in the above example) that points to the load balanced Gateway VIP (see page 29 for details on configuring this VIP)

• If using multiple connection brokers, ensure that the HA settings are configured correctly within the Deployment Properties:

The DNS round robin name (rdscb.robstest.com in the above example) 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 (see page 32 for details on configuring this VIP)

• Ensure that the Remote Authorization Policy policies permits connections to the session host servers and the DNS round robin HA name (if HA mode is used) as shown below:
• Ensure that all load balanced gateway servers are members of the same RD Gateway server farm as shown in the example below:

**APPLIANCE 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 HTTPS VIRTUAL SERVICE (VIP)**

1. Using the WebUI, navigate to: Cluster Configuration > Layer 7 – Virtual Services and click Add a New Virtual Service
2. Enter the following details:
### Load Balancing Gateways (Scenario 5)

#### Setting Up Virtual Services

1. Enter an appropriate name (Label) for the Virtual Service, e.g. **GW-Cluster-TCP**
2. Set the **Virtual Service IP address** field to the required IP address, e.g. **192.168.2.120**
3. Set the **Virtual Service Ports** field to **443**
4. Set the **Layer 7 Protocol** to **TCP Mode**
5. Click **Update**
6. Now click **Modify** next to the newly created Virtual Service
7. Ensure **Persistence Mode** is set to **Source IP**
8. Set the **Persistence Timeout** to **120** (i.e. 2 hours)
9. Enable (check) the **Timeout** checkbox and set both **Client & Real Server Timeout** to **2h** (i.e. 2 hours)
10. Click **Update**

#### Setting Up the Real Servers (RIPS)

1. Using the WebUI, navigate to: **Cluster Configuration > Layer 7 – Real Servers** and click **Add a New Real Server** next to the newly created Virtual Service
2. Enter the following details:

<table>
<thead>
<tr>
<th>Label</th>
<th>GW1</th>
</tr>
</thead>
<tbody>
<tr>
<td>Real Server IP Address</td>
<td>192.168.2.220</td>
</tr>
<tr>
<td>Real Server Port</td>
<td>443</td>
</tr>
<tr>
<td>Re-Encrypt to Backend</td>
<td></td>
</tr>
<tr>
<td>Weight</td>
<td>100</td>
</tr>
</tbody>
</table>

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

#### Applying the New Layer 7 Settings

1. Using the WebUI, navigate to: **Cluster Configuration > Layer 7 – Virtual Services** and click **Modify** next to the newly created Virtual Service
2. Enter the following details:

<table>
<thead>
<tr>
<th>Label</th>
<th>GW-Cluster-TCP</th>
</tr>
</thead>
<tbody>
<tr>
<td>Virtual Service IP Address</td>
<td>192.168.2.120</td>
</tr>
<tr>
<td>Ports</td>
<td>443</td>
</tr>
<tr>
<td>Layer 7 Protocol</td>
<td>TCP Mode</td>
</tr>
</tbody>
</table>

3. Enter an appropriate name (Label) for the Virtual Service, e.g. **GW-Cluster-TCP**
4. Set the **Virtual Service IP address** field to the required IP address, e.g. **192.168.2.120**
5. Set the **Virtual Service Ports** field to **443**
6. Set the **Layer 7 Protocol** to **TCP Mode**
7. Click **Update**
8. Now click **Modify** next to the newly created Virtual Service
9. Ensure **Persistence Mode** is set to **Source IP**
10. Set the **Persistence Timeout** to **120** (i.e. 2 hours)
11. Enable (check) the **Timeout** checkbox and set both **Client & Real Server Timeout** to **2h** (i.e. 2 hours)
12. Click **Update**
1. 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)**

1. Using the WebUI, navigate to: *Cluster Configuration > Layer 4 – Virtual Services* and click **Add a New Virtual Service**
2. Enter the following details:

```
<table>
<thead>
<tr>
<th>Label</th>
<th>GW-Cluster-UDP</th>
</tr>
</thead>
<tbody>
<tr>
<td>Virtual Service</td>
<td>192.168.2.120</td>
</tr>
<tr>
<td>IP Address</td>
<td></td>
</tr>
<tr>
<td>Ports</td>
<td>3391</td>
</tr>
<tr>
<td>Protocol</td>
<td>UDP</td>
</tr>
<tr>
<td>Forwarding Method</td>
<td>Direct Routing</td>
</tr>
</tbody>
</table>
```
3. Enter an appropriate name (Label) for the Virtual Service, e.g. **GW-Cluster-UDP**
4. Set the **Virtual Service IP address** field to the required IP address, e.g. **192.168.2.120**
5. Set the **Virtual Service Ports** field to **3391**
6. Set the **Protocol** to **UDP**
7. Set the **forwarding Method** to **Direct Routing**
8. Click **Update**
9. Now click **Modify** next to the newly created Virtual Service
10. Ensure that the **Persistent** check-box is checked (enabled)
11. Click **Update**

**SETTING UP THE UDP REAL SERVERS (RIPS)**

1. Using the WebUI, navigate to: *Cluster Configuration > Layer 4 – Real Servers* and click **Add a New Real Server** next to the newly created Virtual Service
2. Enter the following details:

```
<table>
<thead>
<tr>
<th>Label</th>
<th>GW1</th>
</tr>
</thead>
<tbody>
<tr>
<td>Real Server IP Address</td>
<td>192.168.2.220</td>
</tr>
<tr>
<td>Weight</td>
<td>100</td>
</tr>
<tr>
<td>Minimum Connections</td>
<td>0</td>
</tr>
<tr>
<td>Maximum Connections</td>
<td>0</td>
</tr>
</tbody>
</table>
```

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

**SETTING UP THE CONNECTION BROKER VIRTUAL SERVICE (VIP)**

If more than one connection broker is used in HA mode, an additional VIP is required. Follow the steps in the section titled *Load Balancer Configuration* on page 23, changing the IP address as needed.

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

As mentioned, ensure there is a valid DNS entry for the RD gateway server defined in the deployment settings. In this example is should be the load balanced gateway address: **rd-gateway.robtest.com** pointing to **192.168.2.120**

---

**13. Load Balancing Web Access Servers (Scenario 6)**

Please refer to page 17 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

**APPLIANCE CONFIGURATION**

**SETTING UP THE VIRTUAL SERVICE (VIP)**

1. Using the WebUI, navigate to: *Cluster Configuration > Layer 7 – Virtual Services* and click **Add a New Virtual Service**
2. Enter the following details:
### Load Balancing Web Access Servers (Scenario 6)

#### Setting up the Virtual Service:

<table>
<thead>
<tr>
<th>Label</th>
<th>WA-Cluster</th>
</tr>
</thead>
<tbody>
<tr>
<td>Virtual Service</td>
<td></td>
</tr>
<tr>
<td>IP Address</td>
<td>192.168.2.130</td>
</tr>
<tr>
<td>Ports</td>
<td>80,443</td>
</tr>
<tr>
<td>Layer 7 Protocol</td>
<td>TCP Mode</td>
</tr>
</tbody>
</table>

3. Enter an appropriate name (Label) for the Virtual Service, e.g. **WA-Cluster**
4. Set the Virtual Service IP address field to the required IP address, e.g. **192.168.2.130**
5. Set the Virtual Service Ports field to **80,443**
6. Set the Layer 7 Protocol to **TCP Mode**
7. Click **Update**
8. Now click **Modify** next to the newly created Virtual Service
9. Ensure Persistence Mode is set to **Source IP**
10. Set Persistence Timeout to an appropriate value, e.g. **120** (i.e. 2 hours)
11. Enable (check) the Timeout checkbox and set both Client & Real Server Timeout to **2h** (i.e. 2 hours)
12. Click **Update**

#### Setting up the Real Servers (RIPS):

1. Using the WebUI, navigate to: Cluster Configuration > Layer 7 – Real Servers and click **Add a New Real Server** next to the newly created Virtual Service
2. Enter the following details:

<table>
<thead>
<tr>
<th>Label</th>
<th>WA1</th>
</tr>
</thead>
<tbody>
<tr>
<td>Real Server IP Address</td>
<td>192.168.2.230</td>
</tr>
<tr>
<td>Real Server Port</td>
<td></td>
</tr>
<tr>
<td>Re-Encrypt to Backend</td>
<td></td>
</tr>
<tr>
<td>Weight</td>
<td>100</td>
</tr>
</tbody>
</table>

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

#### Applying the New Layer 7 Settings
1. 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

14. **Technical Support**

For more details about configuring the appliance and assistance with designing your deployment please don’t hesitate to contact the support team using the following email address: support@loadbalancer.org

15. **Further Documentation**


16. **Conclusion**

Loadbalancer.org appliances provide a very cost effective and flexible solution for highly available load balanced Remote Desktop Services environments.
17. 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**

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

- DR 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 the Real Server 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 page 38 for more details.
- 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

**Note:**

Layer 4 DR mode is used for the Gateway UDP requirement in this guide.
Appendix

LAYER 4 NAT MODE
Layer 4 NAT mode is also a high performance solution, although not as fast as layer 4 DR mode. This is because real server responses must flow back to the client via the load balancer rather than directly as with DR mode.

- 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 WebUI 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’ refer to 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 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 --> RIPv8080 is possible
Layer 7 load balancing uses a proxy (HAProxy) at 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 generally chosen when the network topology prohibits the use of the 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 not need to set the appliance as the gateway.

This mode can be deployed in a one-arm or two-arm configuration and does not require any changes to the Real 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 load balancer proxies the application traffic to the servers so that the source of all traffic becomes the load balancer.

- SNAT mode is a full proxy and therefore load balanced Real Servers do not need to be changed in any way
- Because SNAT mode is a full proxy any server in the cluster can be on any accessible subnet including across the Internet or WAN
- SNAT mode 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 own IP address by default, or any other local appliance IP address if preferred (e.g. the VIP address), this can be configured per layer 7 VIP
- SNAT mode can be deployed using either a 1-arm or 2-arm configuration
2 - SOLVING THE ARP PROBLEM

When using Layer 4 DR mode, the ARP problem must be solved. This involves configuring each Real Server to be able to receive traffic destined for the VIP, and ensuring that each Real Server does not respond to ARP requests for the VIP address – only the load balancer should do this.

The steps below are for Windows 2012 / 2016, for other versions of Windows please refer to chapter 6 in the Administration Manual.

Step 1: Install the Microsoft Loopback Adapter

1. Click **Start**, then run `hdwwiz` 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**.

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

Step 2: Configure the Loopback Adapter

1. Open Control Panel and click **Network and Sharing Center**.
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)** and **Internet Protocol Version 6 (TCP/IPv6)** as shown below:
Note:
Leaving both checked ensures that both IPv4 and IPv6 are supported. Select one if preferred.

5. If configuring IPv4 addresses 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. 192.168.2.20/255.255.255.255 as shown below:
6. If configuring IPv6 addresses select **Internet Protocol Version (TCP/IPv6)**, click **Properties** and configure the IP address to be the same as the Virtual Service (VIP) and set the **Subnet Prefix Length** to be the same as your network setting, e.g. 2001:470:1f09:e72::15/64 as shown below:

![IPv6 Properties](image)

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

8. Now repeat the above process on the other Windows 2012/2016 Real Servers

**Step 3: Configure the strong/weak host behavior**

Windows Server 2000 and Windows Server 2003 use the weak host model for sending and receiving for all IPv4 interfaces and the strong host model for sending and receiving for all IPv6 interfaces. You cannot configure this behavior. The Next Generation TCP/IP stack in Windows 2008 and later supports strong host sends and receives for both IPv4 and IPv6 by default. To ensure that Windows 2012/2016 is running in the correct mode to be able to respond to the VIP, the following commands must be run on each Real Server:

For IPv4 addresses:

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

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

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

For IPv6 addresses:
For these commands to work, the LAN connection NIC must be named “net” and the loopback NIC must be named “loopback” as shown below. 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 ipv6 set interface "LAN" weakhostreceive=enabled
netsh interface ipv6 set interface "LOOPBACK" weakhostreceive=enabled
netsh interface ipv6 set interface "LOOPBACK" weakhostsend=enabled
netsh interface ipv6 set interface "LOOPBACK" dadtransmits=0

Note:
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.

1. Start Powershell or use a command window to run the appropriate netsh commands as shown in the example below:

Note:
This shows an IPv6 example, use the IPv4 commands if you’re using IPv4 addresses.

2. Now repeat these 4 commands on the other Windows 2012 Real Servers

Note:
Solving the ARP problem for other version of Windows is similar. For full details, please refer to the Administration Manual.
3 - SERVER FEEDBACK AGENT

The load balancer can modify the weight (amount of traffic) of each server by gathering data from either a custom agent or an HTTP server. For layer 4 VIPs the feedback method can be set to either agent or HTTP, for Layer 7 VIPs, only the agent method is supported.

A telnet to port 3333 on a Real Server with the agent installed will return the current 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 C:\ProgramData\LoadBalancer.org\LoadBalancer).

The load balancer typically expects a 0–99 integer response from the agent which by default relates to the current CPU idle state, e.g. a response of 92 would imply that the Real Servers CPU is 92% idle. The load balancer will then use the formula (92/100*requested_weight) to find the new optimized weight. Using this method an idle Real Server will get 10 times as many new connections as an overloaded server.

Note:
The ‘Requested Weight’ is the weight set in the WebUI for each Real Server added, the default is 100. 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
Appendix

Select the installation folder and click **Next**

![Select Installation Folder](image)

**Note:**
The agent should be installed on all Real Serves in the cluster.

**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:

1. Using the WebUI, navigate to: *Cluster Configuration > Layer 4 - Virtual Services or Layer 7 - Virtual Services*
2. Click **Modify** next to the Virtual Service

3. Change the Feedback Method to **Agent**
4. Click **Update**
5. For layer 7 VIPs, restart HAProxy using the WebUI option: *Maintenance > Restart Services*
Appendix

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:

1. Open Remote Desktop Host Session Configuration
2. Right-click ‘Member of farm in RD Connection Broker’ and select Properties
3. Click Change Settings
4. 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
5. 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 section below for more details:

Note:
A number of settings are not replicated as part of the master/slave pairing process and therefore must be manually configured on the slave appliance. These are listed below:

- Hostname & DNS settings
- Network settings including IP addresses, bonding configuration and VLANs
- Routing configuration including default gateways and static routes
- Date & time settings
- Physical – Advanced Configuration settings including Internet Proxy IP address & port, Firewall table size, SMTP relay and Syslog server
- SNMP settings
- Graphing settings
- Firewall Script & Firewall Lockdown Script settings
- Software updates
Version 7:

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

Version 8:

To add a slave node – i.e. create a highly available clustered pair:

- Deploy a second appliance that will be the slave and configure initial network settings
- Using the WebUI, navigate to: Cluster Configuration > High-Availability Configuration

![Image of Cluster Configuration](image)

- Specify the IP address and the loadbalancer users password (the default is ‘loadbalancer’) for the slave (peer) appliance as shown above
- Click Add new node
- The pairing process now commences as shown below:

![Image of Pairing Process](image)

- Once complete, the following will be displayed:
• To finalize the configuration, restart heartbeat and any other services as prompted in the blue message box at the top of the screen

Note:
Clicking the **Restart Heartbeat** button on the master appliance will also automatically restart heartbeat on the slave appliance

Note:
Please refer to chapter 9 – Appliance Clustering for HA in the Administration Manual for more detailed information on configuring HA with 2 appliances.
## 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.  
4250 Lancaster Pike, Suite 120  
Wilmington  
DE 19805  
USA  
Tel: +1 888.867.9504  
Fax: +1 302.213.0122  
Email (sales): [sales@loadbalancer.org](mailto:sales@loadbalancer.org)  
Email (support): [support@loadbalancer.org](mailto:support@loadbalancer.org) |
| **North America (Canada)** | Loadbalancer.org Ltd  
300-422 Richards Street  
Vancouver, BC  
V6B 2Z4  
Canada  
Tel: +1 866.998.0508  
Fax: +1 302.213.0122  
Email (sales): [sales@loadbalancer.org](mailto:sales@loadbalancer.org)  
Email (support): [support@loadbalancer.org](mailto:support@loadbalancer.org) |
| **Europe (UK)** | Loadbalancer.org Ltd.  
Compass House  
North Harbour Business Park  
Portsmouth, PO6 4PS  
UK  
Tel: +44 (0)330 3801064  
Fax: +44 (0)870 4327672  
Email (sales): [sales@loadbalancer.org](mailto:sales@loadbalancer.org)  
Email (support): [support@loadbalancer.org](mailto:support@loadbalancer.org) |
| **Europe (Germany)** | Loadbalancer.org GmbH  
Tengstraße 27  
D-80798  
München  
Germany  
Tel: +49 (0)89 2000 2179  
Fax: +49 (0)30 920 383 6495  
Email (sales): [vertrieb@loadbalancer.org](mailto:vertrieb@loadbalancer.org)  
Email (support): [support@loadbalancer.org](mailto:support@loadbalancer.org) |