Load Balancing VMware Horizon

v1.1.2

Deployment Guide
## Contents

1. About this Guide........................................................................................................................................... 4
2. Loadbalancer.org Appliances Supported.................................................................................................. 4
3. Loadbalancer.org Software Versions Supported....................................................................................... 4
4. VMware Horizon Versions Supported......................................................................................................... 5
5. VMware Horizon........................................................................................................................................... 5
6. VMware Horizon Servers to be Load Balanced......................................................................................... 5
7. VMware Horizon Protocols......................................................................................................................... 5
   - Primary Horizon Protocol (Phase 1)........................................................................................................... 6
   - Secondary Horizon Protocol (Phase 2)....................................................................................................... 6
8. Load Balancing VMware Horizon................................................................................................................ 6
   - Port Requirements................................................................................................................................... 7
   - Persistence (aka Server Affinity)................................................................................................................ 7
   - SSL Certificates......................................................................................................................................... 7
   - SSL Offload................................................................................................................................................. 8
   - Load Balancer Deployment Modes........................................................................................................... 8
   - Server Health Checks............................................................................................................................... 8
9. Load Balancer Deployment Options............................................................................................................ 8
   - External Clients......................................................................................................................................... 9
   - External Clients – Option 1....................................................................................................................... 9
   - External Clients – Option 2....................................................................................................................... 10
   - External Clients – Option 3..................................................................................................................... 11
   - Internal Clients......................................................................................................................................... 12
10. Network Topology Used for this Guide...................................................................................................... 12
11. Loadbalancer.org Appliance – the Basics................................................................................................. 13
   - Virtual Appliance Download & Deployment........................................................................................... 13
   - Initial Network Configuration.................................................................................................................... 13
   - Accessing the Web User Interface (WebUI).............................................................................................. 13
   - HA Clustered Pair Configuration............................................................................................................... 14
12. Configuring for External Clients................................................................................................................ 15
   - Option 1.................................................................................................................................................... 15
     - Connection Server Configuration.......................................................................................................... 15
     - UAG Configuration............................................................................................................................... 16
     - Load Balancer Configuration................................................................................................................ 17
   - Option 2.................................................................................................................................................... 19
     - Connection Server Configuration.......................................................................................................... 20
     - UAG Configuration............................................................................................................................... 20
     - Load Balancer Configuration................................................................................................................ 21
   - Option 3.................................................................................................................................................... 26
     - Connection Server Configuration.......................................................................................................... 26
     - UAG Configuration............................................................................................................................... 26
     - Load Balancer Configuration................................................................................................................ 28
13. Configuring for Internal Clients................................................................................................................. 31
   - Connection Server Configuration............................................................................................................ 31
Load Balancer Configuration .................................................................................................................................................................................................................................................31
Configuring The VIP & RIPs for the Primary Protocol (source IP persistence) ..........................................................32
Configuring the VIP & RIPs for the Primary Protocol (Cookie persistence) ..........................................................33
Configure Remaining Load Balancer Settings & Reload Services ..................................................................................36
14. Testing & Verification ..............................................................................................................................................................................................................................................37
    Client Protocol Testing ..................................................................................................................................................................................................................................................37
    Using System Overview .................................................................................................................................................................................................................................37
Layer 4 Current Connections Report ........................................................................................................................................................................................................................................38
Layer 4 Status Report ................................................................................................................................................................................................................................................................38
Layer 7 Statistics Report ................................................................................................................................................................................................................................................................38
    Appliance Logs ..................................................................................................................................................................................................................................................................39
15. Technical Support ..................................................................................................................................................................................................................................................................39
16. Further Documentation .................................................................................................................................................................................................................................39
17. Conclusion ..................................................................................................................................................................................................................................................................39
18. Appendix ..................................................................................................................................................................................................................................................................40
    1 – Configuring an HTTP to HTTPS redirect ..........................................................................................................................40
    2 – Clustered Pair Configuration – Adding a Slave Unit ..........................................................................................................................40
19. Document Revision History ..................................................................................................................................................................................................................................................................43

© Copyright LoadBalancer.org • www.loadbalancer.org • sales@loadbalancer.org
1. About this Guide
This guide details the steps required to configure a load balanced VMware Horizon environment utilizing Loadbalancer.org appliances. It covers the configuration of the load balancers and also any VMware Horizon configuration changes that are required to enable load balancing.

Note: If you want to load balance VMware Horizon v6.1 & earlier (with Security Server) please refer to this guide.

For more information about initial appliance deployment, network configuration and using the Web User Interface (WebUI), please also refer to the relevant Administration Manual:

- v7 Administration Manual
- v8 Administration Manual

2. Loadbalancer.org Appliances Supported
All our products can be used with VMware Horizon. 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 40G</td>
</tr>
<tr>
<td></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>
<tr>
<td></td>
<td>Enterprise GCP **</td>
</tr>
</tbody>
</table>

* For full specifications of these models please refer to: http://www.loadbalancer.org/products/hardware

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

3. Loadbalancer.org Software Versions Supported

- v8.3.1 and later
4. VMware Horizon Versions Supported

- v6.2 & later

5. VMware Horizon

VMware Horizon (formerly VMware Horizon View) is a virtual desktop infrastructure (VDI) solution that simplifies desktop management and provides users with access to these desktops when needed, from virtually any device, whatever their location.

6. VMware Horizon Servers to be Load Balanced

<table>
<thead>
<tr>
<th>Server</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Connection Server</td>
<td>Horizon Connection Server acts as a broker for client connections by authenticating and then directing incoming user requests to the appropriate remote desktops and applications.</td>
</tr>
<tr>
<td>Security Server</td>
<td>A security server is an instance of a Connection Server that is installed in the DMZ. It adds an additional layer of security between the Internet and the internal network. Each Security Server must be paired with a Connection Server and forwards all traffic to that instance.</td>
</tr>
</tbody>
</table>

Note: Security Server is still developed and supported and can be used instead of Unified Access Gateway. However, some of the newer Blast functionality only works in Unified Access Gateway.

<table>
<thead>
<tr>
<th>Access Point</th>
<th>Access Point is a hardened Linux based appliance introduced in v6.2 as an alternative to Security Server.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Unified Access Gateway</td>
<td>Access Point was renamed Unified Access Gateway in Horizon v7.0. UAG is now the preferred option over Security Server.</td>
</tr>
</tbody>
</table>

Note: This guide demonstrates how to load balance Connection Servers and Unified Access Gateways.

7. VMware Horizon Protocols

When a VMware Horizon Client user connects to a Horizon environment, several different protocols are used. The first connection is always the primary XML-API protocol over HTTPS. Following successful authentication, one or more secondary protocols are also made.
Primary Horizon Protocol (Phase 1)
The user enters a hostname at the Horizon Client and this starts the primary Horizon protocol. This is a control protocol for authentication, authorization and session management. It uses XML structured messages over HTTPS. This protocol is sometimes known as the Horizon XML-API control protocol. In a load balanced environment, the load balancer distributes client connections across the available set of UAGs.

Secondary Horizon Protocols (Phase 2)
After the Horizon Client has established secure communication to one of the UAG appliances, the user authenticates. If this authentication attempt is successful, then one or more secondary connections are made from the Horizon client. These secondary connections can include:

- HTTPS Tunnel used for encapsulating TCP protocols such as RDP, MMR/CDR and the client framework channel (TCP 443)
- Blast display protocol (TCP/UDP 443 & TCP/UDP 8443)
- PCoIP display protocol (TCP/UDP 4172)

These secondary Horizon protocols must be routed to the same UAG appliance to which the primary Horizon protocol was routed. The reason for this is so that UAG can authorize the secondary protocols based on the authenticated user session. If the secondary protocols were to be misrouted to a different UAG appliance to the primary protocol one, they would not be authorized and would therefore be dropped in the DMZ and the connection would fail.

8. Load Balancing VMware Horizon

Note: It's highly recommended that you have a working VMware Horizon environment first before implementing the load balancer.

The diagram below illustrates where the load balancers are positioned in a typical deployment. With the older VMware Horizon View architecture, each Security Server had to be paired with a Connection Server. This pairing required the Connection Server to be in tunnel mode, which meant it was not suitable for internal client connections, so two sets of Connection Servers were needed. UAG is not paired, so only one set of Connection Servers is needed for both external and internal clients.
Notes: We recommend that a clustered pair of load balancers is deployed rather than a single appliance to avoid introducing a single point of failure.

Port Requirements
The following table shows the ports that are load balanced:

<table>
<thead>
<tr>
<th>Port</th>
<th>Transport Protocol</th>
<th>Use</th>
</tr>
</thead>
<tbody>
<tr>
<td>443</td>
<td>TCP</td>
<td>Various HTTPS traffic</td>
</tr>
<tr>
<td>443</td>
<td>TCP &amp; UDP</td>
<td>Blast</td>
</tr>
<tr>
<td>4172</td>
<td>TCP &amp; UDP</td>
<td>PCoIP</td>
</tr>
<tr>
<td>8443</td>
<td>TCP &amp; UDP</td>
<td>Blast</td>
</tr>
</tbody>
</table>

Note: Some of the above ports may not be used in all scenarios. For simplicity when setting up the load balancer, and to ensure all scenarios are covered, all are included.

For full details of ports used under various scenarios, please refer to the following URLs:

TCP and UDP Ports Used by Clients and Agents
UAG Documentation Reference

Persistence (aka Server Affinity)

External Clients
Source IP address or cookie based persistence can be used to ensure all primary protocol connections are handled by the same UAG. For simplicity, source IP address persistence is recommended where possible. Typically, the only time source IP persistence is not appropriate is when clients are located behind a NAT device that hides their IP addresses. Secondary protocol connections must be handled by the same UAG to which the primary protocol was routed. This can be achieved in various ways as described on page 8.

Internal Clients
Source IP address or cookie based persistence can be used to ensure all primary protocol connections are handled by the same Connection Server. For simplicity, source IP address persistence is recommended where possible. Typically, the only time source IP persistence is not appropriate is when clients are located behind a NAT device that hides their IP addresses. Secondary protocol connections are direct from client to Connection Server.

SSL Certificates
Wild card certificates and SAN based certificates are supported for VMware Horizon. In this guide, the SSL certificate was obtained from an internal CA. The common name was set to horizon.lbtestdom.com and SANs were added for the hostname of each Connection Server and UAG. For more information on using, configuring and troubleshooting SSL
certificates for Horizon servers, please refer to the following links: Configuring SSL Certificates for Horizon 7 Servers, Setting Up SSL Certificates for Horizon.

SSL Offload
Terminating SSL on the load balancer is only necessary when using cookie based persistence for the primary protocol connections. Cookie based persistence is only needed when source IP address persistence cannot be used due to inline NAT/proxy devices hiding client source IP addresses. If SSL offload is used, the load balancer and the UAGs must have the same certificate as mentioned here.

Load Balancer Deployment Modes
The primary protocol is TCP/HTTPS based, so either layer 7 or layer 4 methods can be used. The secondary protocols use both TCP & UDP so only layer 4 methods are supported. Layer 4 NAT mode and layer 7 SNAT mode are used for the configurations presented in this guide.

Note: Layer 4 DR mode is not supported for UAG. This is because UAG is a hardened appliance based on Linux which has been locked down by VMware. This means that modifying the UAGs to solve the ARP issue becomes more complex and may cause unforeseen issues.

Server Health Checks
The load balancer is configured to check the health of each Connection Server and UAG by periodically sending an HTTPS GET /favicon.ico request. It will perform this HTTPS GET and expect a "200 OK" response. If it receives a response other than "200 OK" or doesn't get any response, that server will be marked as down and will not attempt to route client requests to it. It will continue to poll so that it can detect when it is available again.

9. Load Balancer Deployment Options
The load balancer can be configured in various ways to support internal and external clients.

External Clients
For external clients, the key requirement as explained on page 6 is that the secondary protocols must be sent to the same UAG as the primary protocol. This guide presents 3 options to achieve this. These are explained below. Please also refer to this VMware URL for additional information.
External Clients – Option 1

The load balancer uses a single VIP configured with source IP address persistence to load balance the primary protocol to one of the UAGs. The client connection URLs on each UAG (page 16) are configured so that secondary protocols are also sent to the VIP for load balancing to the same UAG.

This option is recommended for all environments where source IP address persistence is possible. Where it’s not possible (typically due to in-line NAT devices hiding client source IP addresses), then either option 2 or option 3 should be used.

Key Points

- Requires a single public IP address
- All traffic passes via the load balancer

Notes:

- The load balancer requires one network interface
- The UAGs are configured with 2 NICs
- The VIP is configured in Layer 4 NAT mode using source IP persistence
- The default gateway of the UAGs must be the load balancer, for a clustered pair of load balancers (master & slave) this should be a floating IP address to allow failover
- The default gateway of the load balancer is the external firewall
- See the steps starting on page 15 for UAG and load balancer configuration guidance
External Clients – Option 2
The load balancer uses a single VIP configured with either source IP address or cookie persistence to load balance the primary protocol to one of the UAGs. The client connection URLs on each UAG (page 20) are configured so that secondary protocols are sent directly to the same UAG, bypassing the load balancer.

Key Points

• Requires multiple public IP addresses – one for the VIP, one for each UAG
• Only the primary protocol is load balanced, secondary protocols go direct to the UAGs

Notes:

• The load balancer requires one network interface
• The UAGs are configured with 2 NICs
• The VIP is configured in Layer 7 SNAT mode using either source IP address or cookie based persistence
• The default gateway of the UAGs is the external firewall
• The default gateway of the load balancer is the external firewall
• See the steps starting on page 19 for UAG and load balancer configuration guidance
External Clients – Option 3

The load balancer uses one VIP configured with either source IP address or cookie persistence to load balance the primary protocol to one of the UAGs. The client connection URLs on each UAG (page 26) are configured so that secondary protocols are sent to the same UAG via additional VIPs on unique port numbers.

Key Points

- Requires a single public IP address (VIP1 – VIP7 use the same IP address)
- All traffic passes via the load balancer
- Uses non standard ports for external client connections (example ports are shown, any appropriate ports can be used)

Notes:

- The load balancer requires one network interface
- The UAGs are configured with 2 NICs
- VIP1 is configured in Layer 7 SNAT mode using either source IP address or cookie based persistence
- VIPs 2 to 7 are configured in Layer 4 NAT mode
- The default gateway of the UAGs must be the load balancer, for a clustered pair of load balancers (master & slave) this should be a floating IP address to allow failover
- The default gateway of the load balancer is the external firewall
- See the steps starting on page 26 for UAG and load balancer configuration guidance
Internal Clients

Internal clients connect directly to the Connection Servers located on the LAN.

Key Points

• Only the primary protocol is load balanced, secondary protocols go direct to the virtual desktops

Notes:

• The load balancer requires one interface
• The VIP is configured in Layer 7 SNAT mode using either source IP address or cookie based persistence
• See the steps starting on page 31 for server and load balancer configuration guidance

10. Network Topology Used for this Guide

The diagram below shows the network topology used for this deployment guide. Clustered Pair 1 in the DMZ is used to load balance external clients connecting to the UAGs, and clustered Pair 2 on the LAN is used to load balance internal clients connecting to the Connection Servers.
11. 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: https://192.168.2.21:9443
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

Accessing the Web User Interface (WebUI)

1. Browse to the following URL: https://192.168.2.21:9443/lbadmin/
(replace with your IP address if it’s been changed)

* Note the port number → 9443

2. Login to the WebUI:
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 below:

**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 2 of the Appendix on page 40.
12. Configuring for External Clients

Option 1
The configuration presented in this section relates to the topology described on page 9.

Connection Server Configuration
For each Connection Server, complete the following steps:

Step 1 – Configure General Settings

Un-check the 3 boxes as shown above. These options are not required when using UAG. These options only need to be set when a security server is paired with the Connection Server.

Step 2 - Enable HTML Access via the Load Balancer
Connection Servers that are directly behind a load balancer or load-balanced gateway must know the address by which browsers will connect to the load balancer when users use HTML Access. On each UAG complete the following steps:

1. Create or edit the `locked.properties` file in the SSL gateway configuration folder, i.e.:
   ```
   software Install folder\VMware\VMware View\Server\sslgateway\conf\locked.properties
   ```
2. Add the **balancedHost** property and set it to the address that users type for HTML Access. For example, if users type `https://horizon.example.com`, add the following entry to the file:

```
balancedHost=horizon.example.com   ( Note: balancedHost is case sensitive! )
```

3. Save the **locked.properties** file

4. Restart the Connection Server service to apply the changes

If the above steps are not completed, you'll receive the following error when connecting via a browser:

```
Error

Failed to connect to the Connection Server.
```

### UAG Configuration

**Horizon Settings**

- **Enable Horizon**: YES
- **Connection Server URL**: https://192.168.112.206
- **Connection Server URL Thumbprint**: sha1=bc07f38554a9e2c43a227024e850b8fdd8e84
- **Enable PCOIP**: YES
- **PCOIP External URL**: 10.208.251.206:4172
- **Enable Blast**: YES
- **Blast External URL**: https://horizon.ibetstdom.com:8443
- **BSG UDP Tunnel Server**: YES
- **Enable Tunnel**: YES
- **Tunnel External URL**: https://horizon.ibetstdom.com:443

**More**

### Step 1 – Configure URLs

The various URLs must be configured on each UAG as shown above. To access the UAG Web Interface use:

```
https://<uag-ip>:9443/admin
```

1. Configure the Connection Server URL to be the VIP address of the load balanced Connection Servers on the
internal load balancer, in this guide https://192.168.112.206

2. Configure the PCoIP External URL to be the public IP address of the VIP on the load balancer, in this guide 10.200.251.206:4172

3. Configure the Blast External URL to be the FQDN that external clients use to connect, in this guide https://horizon.lbtestdom.com:8443, this should resolve to the public IP address of the VIP on the load balancer

4. Configure the Tunnel External URL to be the FQDN that external clients use to connect, in this guide https://horizon.lbtestdom.com:443, this should resolve to the public IP address of the VIP on the load balancer

Note: Steps 2 – 4 above illustrate that clients connect via the load balancer for all secondary protocols.

Step 2 - Configure the Default Gateway on the UAGs

Note: Return traffic MUST pass back via the load balancer for layer 4 NAT mode to operate.

1. Set the default gateway on each UAG to be an address on the load balancer. This address should be a floating IP address to enable failover when using a clustered pair as described in the Load Balancer Configuration section (Step 2) below.

Note: The default gateway can be set at UAG deployment, or later by using the UAG’s Admin UI as mentioned here.

Load Balancer Configuration
The load balancer is used for both the primary and secondary protocols.

Port Requirements
The following table shows the ports that are load balanced:

<table>
<thead>
<tr>
<th>Port</th>
<th>Transport Protocol</th>
<th>Use</th>
</tr>
</thead>
<tbody>
<tr>
<td>443</td>
<td>TCP</td>
<td>Various HTTPS traffic</td>
</tr>
<tr>
<td>443</td>
<td>TCP &amp; UDP</td>
<td>Blast</td>
</tr>
<tr>
<td>4172</td>
<td>TCP &amp; UDP</td>
<td>PCoIP</td>
</tr>
<tr>
<td>8443</td>
<td>TCP &amp; UDP</td>
<td>Blast</td>
</tr>
</tbody>
</table>
Step 1 - Configure the Virtual Service & Real Servers

a) Setting up the Virtual Service

1. Using the WebUI, navigate to: Cluster Configuration > Layer 4 – Virtual Service and click Add a New Virtual Service
2. Enter the following details:
   - Enter an appropriate label (name) for the VIP, e.g. HorizonExternal
   - Set the Virtual Service IP address field to the required IP address, e.g. 10.200.251.206
   - Set the Virtual Service Ports field to 443,4172,8443
   - Set the Protocol to TCP/UDP
   - Set the Forwarding Method to NAT
   - Click Update
   - Now click Modify next to the newly created VIP
   - Ensure Persistence is enabled and set Persistence Timeout to 36000 (i.e. 10 hour)

   Note: As mentioned [here](#), the value set should match the Forcibly disconnect users setting under Global Settings for the Connection Server (the default value for this is 10 hours).

3. Set Check Type to Negotiate
4. Set Check Port to 443
5. Set Protocol to HTTPS
6. Set Request to send to favicon.ico
7. Leave Response expected blank
8. Click Update

b) Setting up the Real Servers
1. Using the WebUI, navigate to: Cluster Configuration > Layer 4 – Real Servers and click Add a New Real Server next to the newly created VIP

2. Enter the following details:

   ![Real Server Configuration](image)

   3. Enter an appropriate label for the RIP, e.g. UAG1
   4. Change the Real Server IP Address field to the required IP address, e.g. 10.200.251.10
   5. Leave the Real Server Port field blank
   6. Click Update
   7. Repeat the above steps to add your other UAG(s)

**Step 2 - Add a Floating IP Address to the Load Balancer to be used as the UAGs Default Gateway**

Using the WebUI option: Cluster Configuration > Floating IP's add a Floating IP that can be used as the default gateway for the UAGs. Using a floating IP will ensure that the IP address is available when a clustered pair is used, and a failover to the slave has occurred. This floating IP should be an additional IP address that is dedicated to this purpose.

**Step 3 - Configure the Default Gateway on the Load Balancer**

Using the WebUI option: Local Configuration > Routing set the default gateway to be the internal interface of the external firewall, e.g. 10.200.251.254

**Step 4 - Configure HTTP to HTTPS Redirection**

If required, the load balancer can be configured to automatically redirect clients who attempt to connect to http://<Horizon URL> to https://<Horizon URL>.

When SSL is terminated on the real servers, a separate VIP is required to handle this. For details on setting this up, please refer to section 1 in the Appendix on page 40.

**Option 2**

The configuration presented in this section relates to the topology described on page 10.
Connection Server Configuration
Follow the Connection Server configuration steps on page 15.

UAG Configuration

Step 1 – Configure URLs
The various URLs must be configured on each UAG as shown above. To access the UAG Web Interface use: https://<uag-ip>:9443/admin

1. Configure the Connection Server URL to be the VIP address of the load balanced Connection Servers on the internal load balancer, in this guide https://192.168.112.206

2. Configure the PCoIP External URL to be the public IP address of the UAG, in this guide 10.200.251.10:4172

3. Configure the Blast External URL to be the FQDN of the UAG, in this guide https://uag1.lbtestdom.com:8443, this should resolve to the public IP address of the UAG

4. Configure the Tunnel External URL to be the FQDN of the UAG, in this guide https://uag1.lbtestdom.com:443, this should resolve to the public IP address of the UAG
Note: Steps 2 – 4 above illustrate that clients connect directly to the UAGs for all secondary protocols, bypassing the load balancer. Using FQDNs for steps 3 & 4 rather than IP addresses avoids certificate related errors. For a SAN certificate, make sure you include the FQDN of each UAG.

Step 2 - Configure the default gateway on the UAGs

1. Set the default gateway on each UAG to be the external firewall.

Note: The default gateway can be set at UAG deployment, or later by using the UAG's Admin UI as mentioned [here](#).

Load Balancer Configuration

The load balancer is used for the primary protocol only, secondary protocols pass directly from client to the UAGs. Source IP address persistence is recommended if there are no inline NAT devices between the clients and the VIP – see the section below for configuration steps. If there are inline NAT devices, cookie based persistence can be used – please see page 23.

Port Requirements

The following table shows the ports that are load balanced:

<table>
<thead>
<tr>
<th>Port</th>
<th>Transport Protocol</th>
<th>Use</th>
</tr>
</thead>
<tbody>
<tr>
<td>443</td>
<td>TCP</td>
<td>Various HTTPS traffic</td>
</tr>
</tbody>
</table>

Configuring the VIP & RIPs for the Primary Protocol (using source IP persistence)

a) Setting up the Virtual Service

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 label for the VIP, e.g. **HorizonExternal**
4. Set the Virtual Service IP address field to the required IP address, e.g. **10.200.251.206**
5. Set the Virtual Service Ports field to **443**
6. Set Layer 7 Protocol to **TCP Mode**
7. Click **Update**
8. Now click **Modify** next to the newly created VIP
9. Set Health Checks to **Negotiate HTTPS**
10. Set Check Port to **443**
11. Set Request to send to **favicon.ico**
12. Leave Response expected blank
13. Click **Update**

b) Setting up the Real Servers

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

3. Enter an appropriate label for the RIP, e.g. **UAG1**
4. Change the **Real Server IP Address** field to the required IP address, e.g. **10.200.251.10**
5. Change the **Real Server Port** field to **443**
6. Click **Update**
7. Repeat the above steps to add your other UAG(s)

### Configuring the VIP & RIPs for the Primary Protocol (using cookie persistence)

**a) Setting up the Virtual Service**

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

```
<table>
<thead>
<tr>
<th>Label</th>
<th>HorizonExternal</th>
</tr>
</thead>
<tbody>
<tr>
<td>Virtual Service IP Address</td>
<td>10.200.251.206</td>
</tr>
<tr>
<td>Ports</td>
<td>80</td>
</tr>
<tr>
<td>Layer 7 Protocol</td>
<td>HTTP Mode</td>
</tr>
</tbody>
</table>
```

3. Enter an appropriate label for the VIP, e.g. **HorizonExternal**
4. Set the **Virtual Service IP address** field to the required IP address, e.g. **10.200.251.206**
5. Set the **Virtual Service Ports** field to **80**
6. Leave **Layer 7 Protocol** set to **HTTP Mode**
7. Click **Update**
8. Now click **Modify** next to the newly created VIP
9. Set **Health Checks** to **Negotiate HTTP**
10. Set **Check Port** to **80**
11. Set **Request to send** to **favicon.ico**
12. Leave **Response expected** blank
13. Click **Update**

**b) Setting up the Real Servers**

1. Using the WebUI, navigate to: *Cluster Configuration > Layer 7 – Real Servers* and click **Add a New Real Server** next to the newly created VIP
2. Enter the following details:
3. Enter an appropriate label for the RIP, e.g. **UAG1**

4. Set the **Real Server IP Address** field to the required IP address, e.g. **10.200.251.10**

5. Set the **Real Server Port** field to **443**

6. Enable (check) **Re-Encrypt to Backend**

7. Click **Update**

8. Repeat the above steps to add your other UAG(s)

c) Configure SSL Termination – Upload the SSL certificate

1. Using the WebUI, navigate to: **Cluster Configuration > SSL Certificate**

2. Click **Add a new SSL Certificate**

3. Select **Upload prepared PEM/PFX file**

4. Enter a suitable label (name) for the certificate, e.g. **Horizon**

5. Browse to the relevant Horizon PFX certificate file

   **Note:** When SSL re-encryption (SSL bridging) is used, the UAG & load balancer **must** have the same SSL certificate as mentioned [here](#).

6. Enter the relevant **PFX File Password**

7. Click **Add Certificate**

d) Configure SSL Termination – Create the SSL Virtual Service

1. Navigate to: **Cluster Configuration > SSL Termination**

2. Click **Add a new Virtual Service**

for v8.3.3 and later:

1. Enter the following details:
2. Enter a suitable Label (name) for the VIP, e.g. SSL
3. Set Associated Virtual Service to the Layer 7 VIP created earlier, e.g. HorizonExternal
4. Leave Virtual Service Port set to 443
5. Leave SSL Operation Mode set to High Security
6. Select the SSL certificate uploaded previously using the SSL Certificate drop-down
7. Click Update

for v8.3.2 and earlier:
1. Enter the following details:

2. Enter the required Label (name) for the Virtual Service, e.g. SSL
3. Select the certificate uploaded previously using the SSL Certificate drop-down
4. Set the Virtual Service IP address to be the same as the VIP created previously, e.g. 10.200.251.206
5. Set the Virtual Service Port field to 443
6. Set the Backend Virtual Service IP address to be the same as the VIP created previously, e.g. 10.200.251.206
7. Set the Backend Virtual Service Port field to 80
8. The other settings can be left at their default values
9. Click Update
Configure Remaining Load Balancer Settings & Reload Services

Step 1 - Configure HTTP to HTTPS Redirection
If required, the load balancer can be configured to automatically redirect clients who attempt to connect to http://<Horizon URL> to https://<Horizon URL>.

- When using cookie based persistence (SSL is terminated on the load balancer), this can be configured by modifying the HorizonExternal VIP and enabling the Force to HTTPS option
- When using source IP persistence (SSL is terminated on the real servers), a separate VIP is required to handle this. For details on setting this up, please refer to section 1 in the Appendix on page 40

Step 2 - Configure the Default Gateway on the Load Balancer
Using the WebUI option: Local Configuration > Routing set the default gateway to be the internal interface of the external firewall, e.g. 10.200.251.254

Step 3 – Reload Services
To apply the new settings, reload HAProxy and STunnel (if using SSL offload) using the Reload buttons in the blue commit changes box at the top of the screen.

Option 3
The configuration presented in this section relates to the topology described on page 11.

Connection Server Configuration
Follow the Connection Server configuration steps on page 15.

UAG Configuration

Step 1 - Decide on the External Ports for the VIPs
The table below shows one possible option for the external ports for the VIPs used for the secondary protocols.

<table>
<thead>
<tr>
<th>VIP/External Port</th>
<th>Primary/Secondary</th>
<th>Protocol</th>
<th>VIP Name</th>
<th>Real Server IP/Port</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>UAG 1 &amp; 2 – Primary Protocol</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>10.200.251.20:443</td>
</tr>
<tr>
<td><strong>UAG1 – Secondary Protocols</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**UAG2 – Secondary Protocols**


---

### Horizon Settings

- **Enable Horizon**: Yes
- **Connection Server URL**: https://192.168.112.206
- **Connection Server URL Thumbprint**: sha1=8c0d6867b596214a3d27a024e6505bf50e8e94
- **Enable PCoIP**: Yes
- **PCoIP External URL**: 10.200.251.206:14172
- **Enable Blast**: Yes
- **Blast External URL**: https://horizon.lbtestdom.com:18443
- **BSG UDP Tunnel Server**: Yes
- **Enable Tunnel**: Yes
- **Tunnel External URL**: https://horizon.lbtestdom.com:1443

**Step 2 – Configure URLs**

The various URLs must be configured on each UAG as shown above. To access the UAG Web Interface use: https://<uag-ip>:9443/admin

1. Configure the **Connection Server URL** to be the VIP address of the load balanced Connection Servers on the internal load balancer, in this guide https://192.168.112.206

2. Configure the **PCoIP External URL** to be the public IP address of the VIP on the load balancer, in this guide 10.200.251.206:4172

3. Configure the **Blast External URL** to be the FQDN that external clients use to connect, in this guide https://horizon.lbtestdom.com:18443, this should resolve to the public IP address of the VIP on the load balancer
4. Configure the **Tunnel External URL** to be the FQDN that external clients use to connect, in this guide [https://horizon.lbtestdom.com:1443](https://horizon.lbtestdom.com:1443), this should resolve to the public IP address of the VIP on the load balancer.

   Note: Steps 2 – 4 above illustrate that clients connect to the VIP on the load balancer for all secondary protocols.

**Step 3 - Configure the default gateway on the UAGs**

   Note: Return traffic MUST pass back via the load balancer for layer 4 NAT mode to operate.

1. Set the default gateway on each UAG to be an address on the load balancer. This address should be a floating IP address to enable failover when using a clustered pair as described in the *Load Balancer Configuration / Configure Remaining Load Balancer Settings & Reload Services (Step 1)* section on page 30.

   Note: The default gateway can be set at UAG deployment, or later by using the UAG's admin UI as mentioned [here](#).

---

**Load Balancer Configuration**

The load balancer is used for both the primary & secondary protocols.

**Configuring the VIP & RIPs for the Primary Protocol**

Source IP address persistence is recommended if there are no inline NAT devices between the clients and the VIP – please follow the steps in the section *Configuring the VIPs & RIPs for the Primary Protocol (using source IP persistence)* on page 21.

If there are inline NAT devices, cookie based persistence can be used – please follow the steps in the section *Configuring the VIPs & RIPs for the Primary Protocol (using Cookie persistence)* on page 23.

Once complete, configure the VIPs for the secondary protocols.

**Configuring the VIPs & RIPs for the Secondary Protocols**

The 6 secondary protocol VIPs (3 for UAG1, 3 for UAG2) listed in the table on page 26 must now be configured.

The configuration for the first VIP, **UAG1-HTTPS** is shown below:

a) Setup the Virtual Service

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

2. Enter the following details:

<table>
<thead>
<tr>
<th>Label</th>
<th>UAG1-443</th>
</tr>
</thead>
<tbody>
<tr>
<td>Virtual Service</td>
<td>10.200.251.206</td>
</tr>
<tr>
<td>Ports</td>
<td>1443</td>
</tr>
<tr>
<td>Protocol</td>
<td>TCP/UDP</td>
</tr>
<tr>
<td>Forwarding Method</td>
<td>NAT</td>
</tr>
</tbody>
</table>

3. Enter an appropriate label (name) for the VIP, e.g. **UAG1-443**
4. Set the **Virtual Service IP address** field to the required IP address, e.g. **10.200.251.206**
5. Set the **Virtual Service Ports** field to **1443**
6. Set the **Protocol** to **TCP/UDP**
7. Set the **Forwarding Method** to **NAT**
8. Click **Update**
9. Now click **Modify** next to the newly created VIP
10. Set **Check Type** to **Negotiate**
11. Set **Check Port** to **443**
12. Set **Protocol** to **HTTPS**
13. Set **Request to send to** to **favicon.ico**
14. Leave **Response expected** blank
15. Click **Update**

b) Setup the Real Servers

1. Using the WebUI, navigate to: **Cluster Configuration > Layer 4 – Real Servers** and click **Add a New Real Server** next to the newly created VIP
2. Enter the following details:
3. Enter an appropriate label for the RIP, e.g. **UAG1**
4. Change the **Real Server IP Address** field to the required IP address, e.g. **10.200.251.10**
5. Set the port to the **443**
6. Click **Update**
7. Repeat the above steps to add your other UAG(s)

Now continue and create the 5 remaining secondary protocol VIPs (UAG1-PCoIP, UAG1-Blast, UAG2-443, UAG2-PCoIP & UAG2-Blast) & associated RIPS listed in the table. Make sure that you:

- Configure all VIPs using layer 4 NAT mode
- Set the **Virtual Service Port** and the **Real Server Port** according to column 1 & 5 respectively in the table
- Set the **Protocol** according to column 3 in the table
- Configure the same health check settings:
  - Set **Check Type** to **Negotiate**
  - Set **Check Port** to **443**
  - Set **Protocol** to **HTTPS**
  - Set **Request to send** to **favicon.ico**
  - Leave **Response expected** blank

With these settings, the load balancer looks for a **200 OK** response from each UAG.

### Configure Remaining Load Balancer Settings & Reload Services

#### Step 1 - Add a Floating IP Address to the Load Balancer to be used as the UAG’s Default Gateway

Using the WebUI option: **Cluster Configuration > Floating IP’s** add a Floating IP that can be used as the default gateway for the UAGs. Using a floating IP will ensure that the IP address is available when a clustered pair is used, and a failover
to the slave has occurred. This floating IP should be an additional IP address that is dedicated to this purpose.

**Step 2 - Configure the Default Gateway on the Load Balancer**

Using the WebUI option: Local Configuration > Routing set the default gateway to be the internal interface of the external firewall, e.g. 10.200.251.254

**Step 3 - Configure HTTP to HTTPS Redirection**

If required, the load balancer can be configured to automatically redirect clients who attempt to connect to \(\text{http://<Horizon URL>}\) to \(\text{https://<Horizon URL>}\).

- When using cookie based persistence (SSL is terminated on the load balancer), this can be configured by modifying the **HorizonExternal** VIP and enabling the **Force to HTTPS** option
- When using source IP persistence (SSL is terminated on the real servers), a separate VIP is required to handle this. For details on setting this up, please refer to section 1 in the Appendix on page 40

**Step 4 – Reload Services**

To apply the new settings, reload HAProxy and STunnel (if using SSL offload) using the **Reload** buttons in the blue commit changes box at the top of the screen.

13. **Configuring for Internal Clients**

The configuration presented in this section relates to the topology described on page 12.

---

Note: Internal clients connect directly to the virtual desktop rather than going via the Connection Servers. For HTML Access, this can result in a Blast certificate error. Please refer to the following URLs for dealing with this: [Blast Certificate Issue](#), [DNS Names for Horizon Servers](#)

---

**Connection Server Configuration**

Follow the Connection Server configuration steps on page 15.

**Load Balancer Configuration**

The load balancer is used for the primary protocol only, secondary protocols pass directly from client to virtual desktop. Source IP address persistence is recommended if there are no inline NAT devices between the clients and the VIP – see the section below for configuration steps. If there are inline NAT devices, cookie based persistence can be used – please see page 33.

---

Note: If you want the actual client IP addresses to be represented in X-Forwarded-For (XFF) headers
which the Connection Servers can use, please follow the section that describes configuring the VIP and RIPv for cookie based persistence on page 33. In addition to the configuration steps mentioned there, you’ll also need to enable (check) the option Set X-Forward-For header when configuring the layer 7 VIP "HorizonInternal". For more information on enabling layer 7 transparency using inserted headers, please refer to the Administration Manual and search for "Using Proxy Protocol & X-Forwarded-For Headers".

Port Requirements
The following table shows the ports that are load balanced:

<table>
<thead>
<tr>
<th>Port</th>
<th>Transport Protocol</th>
<th>Use</th>
</tr>
</thead>
<tbody>
<tr>
<td>443</td>
<td>TCP</td>
<td>Various HTTPS traffic</td>
</tr>
</tbody>
</table>

Configuring The VIP & RIPv For The Primary Protocol (source IP Persistence)

a) Setting up the Virtual Service

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 label for the VIP, e.g. HorizonInternal
4. Set the Virtual Service IP address field to the required IP address, e.g. 192.168.112.206
5. Set the Virtual Service Ports field to 443
6. Set Layer 7 Protocol to TCP Mode
7. Click Update
8. Now click Modify next to the newly created VIP
9. Set Health Checks to Negotiate HTTPS
10. Set Check Port to 443
11. Set Request to send to favicon.ico
12. Leave Response expected blank
13. Click Update

b) Setting up the Real Servers
1. Using the WebUI, navigate to: Cluster Configuration > Layer 7 – Real Servers and click Add a New Real Server next to the newly created VIP
2. Enter the following details:

```
Label: CS1
Real Server IP Address: 192.168.112.200
Real Server Port: 443
Re-Encrypt to Backend: [ ]
Weight: 100
```
3. Enter an appropriate label for the RIP, e.g. CS1
4. Change the Real Server IP Address field to the required IP address, e.g. 192.168.112.200
5. Change the Real Server Port field to 443
6. Click Update
7. Repeat the above steps to add your other Connection Server(s)

Configuring The VIP & RIPS For The Primary Protocol (Cookie Persistence)

a) Setting up the Virtual Service
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 label for the VIP, e.g. HorizonInternal
4. Set the Virtual Service IP address field to the required IP address, e.g. 192.168.112.206
5. Set the Virtual Service Ports field to 80
6. Leave Layer 7 Protocol set to HTTP Mode
7. Click Update
8. Now click Modify next to the newly created VIP
9. Set Health Checks to Negotiate HTTP
10. Set Check Port to 80
11. Set Request to send to favicon.ico
12. Leave Response expected blank
13. Click Update

b) Setting up the Real Servers
1. Using the WebUI, navigate to: Cluster Configuration > Layer 7 – Real Servers and click Add a New Real Server next to the newly created VIP
2. Enter the following details:

   3. Enter an appropriate label for the RIP, e.g. CS1
   4. Change the Real Server IP Address field to the required IP address, e.g. 192.168.112.200
5. Change the Real Server Port field to **443**
6. Click **Update**
7. Repeat the above steps to add your other Connection Server(s)

c) Configure SSL Termination – Upload the SSL certificate
   1. Using the WebUI, navigate to: Cluster Configuration > SSL Certificate
   2. Click **Add a new SSL Certificate**
   3. Select **Upload prepared PEM/PFX file**
   4. Enter a suitable label (name) for the certificate, e.g. **Horizon**
   5. Browse to the relevant Horizon PFX certificate file
   6. Enter the relevant **PFX File Password**
   7. Click **Add Certificate**

d) Configure SSL Termination – Create the SSL Virtual Service
   1. Navigate to: Cluster Configuration > SSL Termination
   2. Click **Add a new Virtual Service**

for v8.3.3 and later:
   1. Enter the following details:

   ![SSL Virtual Service Configuration](image)

   2. Enter a suitable Label (name) for the VIP, e.g. **SSL**
   3. Set **Associated Virtual Service** to the Layer 7 VIP created earlier, e.g. **HorizonInternal**
   4. Leave **Virtual Service Port** set to **443**
   5. Leave **SSL Operation Mode** set to **High Security**
   6. Select the SSL certificate uploaded previously using the SSL Certificate drop-down
   7. Click **Update**

for v8.3.2 and earlier:
1. Enter the following details:

![Virtual Service Configuration Form]

2. Enter the required Label (name) for the Virtual Service, e.g. **SSL**
3. Select the certificate uploaded previously in the SSL Certificate drop-down
4. Set the Virtual Service IP address to be the same as the VIP created previously, e.g. **10.200.251.206**
5. Set the Virtual Service Port field to **443**
6. Set the Backend Virtual Service IP address to be the same as the VIP created previously, e.g. **10.200.251.206**
7. Set the Backend Virtual Service Port field to **80**
8. The other settings can be left at their default values
9. Click **Update**

Configure Remaining Load Balancer Settings & Reload Services

**Step 1 - Configure HTTP to HTTPS Redirection**

If required, the load balancer can be configured to automatically redirect clients who attempt to connect to **http://<Horizon URL>** to **https://<Horizon URL>**.

- When using cookie based persistence (SSL is terminated on the load balancer), this can be configured by modifying the HorizonInternal VIP and enabling the Force to HTTPS option
- When using source IP persistence (SSL is terminated on the real servers), a separate VIP is required to handle this. For details on setting this up, please refer to section 1 in the Appendix on page 40

**Step 2 – Reload Services**

To apply the new settings, reload HAProxy and STunnel (if using SSL offload) using the **Reload** buttons in the blue commit changes box at the top of the screen.
14. Testing & Verification

**Client Protocol Testing**
To ensure that all required client protocols are configured correctly, the Horizon client should be configured to each of the configured protocols using the right-click menu as shown below for both internal and external clients.

![Client Protocol Testing](image)

HTML Access should also be verified for internal and external clients using a browser.

**Using System Overview**
The System Overview shows a graphical view of all VIPs & RIPs (i.e. the Horizon Servers) and shows the state/health of each server as well as the state of the cluster as a whole. The example below shows that both UAGs are healthy and available to accept connections.

![System Overview](image)
Layer 4 Current Connections Report
The Layer 4 Current Connection report shows all current layer 4 connects and their status. This can be accessed in the WebUI using the option: Reports > Layer 4 Current Connections. The example below shows the report whilst an External Horizon Client is connected via a layer 4 VIP.

![Layer 4 Current Connections](image)

Layer 4 Status Report
The Layer 4 Status report gives a summary of layer 4 configuration and running stats as shown below. This can be accessed in the WebUI using the option: Reports > Layer 4 Status.

![Layer 4 Status](image)

Layer 7 Statistics Report
The Layer 7 Statistics report gives a summary of all layer 7 configuration and running stats as shown below. This can be accessed in the WebUI using the option: Reports > Layer 7 Status.
Appliance Logs

Logs are available for both layer 4 and layer 7 services and can be very useful when trying to diagnose issues. Layer 4 logs are active by default and can be accessed using the WebUI option: Logs > Layer 4. Layer 7 logging is not enabled by default (because it's extremely verbose) and can be enabled using the WebUI option: Cluster Configuration > Layer 7 - Advanced Configuration, and then viewed using the option: Logs > Layer 7.

15. Technical Support

If you have any questions regarding the appliance or would like assistance designing your deployment, please don't hesitate to contact our support team: support@loadbalancer.org.

16. Further Documentation


17. Conclusion

Loadbalancer.org appliances provide a very cost effective solution for highly available load balanced VMware Horizon environments.
18. Appendix

1 - Configuring an HTTP to HTTPS redirect
An additional layer 7 VIP is required that listens on HTTP port 80 on the same IP address. The VIP is then configured to redirect connections to HTTPS port 443.

E.g. http://horizon.lbtestdom.com should be redirected to https://horizon.lbtestdom.com

The steps:

1) Create another Layer 7 VIP with the following settings:
   - Label: HTTP-redirect
   - Virtual Service IP Address: <same as the VIP that's listening on port 443>
   - Virtual Service Ports: 80
   - Layer 7 Protocol: HTTP Mode
   - Persistence Mode: None
   - Force to HTTPS: Yes

   Note: This additional VIP will be shown purple/green to indicate that it's being used for HTTP to HTTPS redirection.

2) Apply the new settings – to apply the new settings, HAProxy must be restarted:
   - Using the WebUI, navigate to: Maintenance > Restart Services and click Restart HAProxy

2 – 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

![CREATE A CLUSTERED PAIR](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:
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.
# Document Revision History

<table>
<thead>
<tr>
<th>Version</th>
<th>Date</th>
<th>Change</th>
<th>Reason for Change</th>
<th>Changed By</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.1.0</td>
<td>13 August 2019</td>
<td>Styling and layout</td>
<td>General styling updates</td>
<td>RJC</td>
</tr>
<tr>
<td>1.1.1</td>
<td>7 January 2020</td>
<td>Updated method to change default gateway on UAGs.</td>
<td>Changes in later versions of the UAG's Admin UI.</td>
<td>RJC</td>
</tr>
<tr>
<td>1.1.2</td>
<td>21 July 2020</td>
<td>New title page</td>
<td>Branding update</td>
<td>AH</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Updated Canadian contact details</td>
<td>Change to Canadian contact details</td>
<td></td>
</tr>
</tbody>
</table>
About Loadbalancer.org

Loadbalancer.org's mission is to ensure that its clients' businesses are never interrupted. The load balancer experts ask the right questions to get to the heart of what matters, bringing a depth of understanding to each deployment. Experience enables Loadbalancer.org engineers to design less complex, unbreakable solutions - and to provide exceptional personalized support.