

Load Balancing Hyland OnBase

Version 1.4.0



Table of Contents

1. About this Brief	3
2. Loadbalancer.org Appliances Supported	3
3. Software Versions Supported	3
3.1. Loadbalancer.org Appliance	3
3.2. Hyland OnBase	3
4. Hyland OnBase	3
5. Load Balancing Hyland OnBase	3
5.1. Virtual Service (VIP) Requirements	3
5.2. SSL Termination	4
6. Deployment Concept	4
7. Load Balancer Deployment Methods	4
7.1. Layer 7 SNAT Mode	4
8. Loadbalancer.org Appliance – the Basics	5
8.1. Virtual Appliance	5
8.2. Initial Network Configuration	6
8.3. Accessing the Appliance WebUI	6
Main Menu Options	7
8.4. Appliance Software Update	8
Determining the Current Software Version	8
Checking for Updates using Online Update	8
Using Offline Update	9
8.5. Ports Used by the Appliance	9
8.6. HA Clustered Pair Configuration	10
9. Appliance Configuration for Hyland OnBase	10
9.1. VIP 1 – WebServers	10
Virtual Service Configuration	10
Define the Associated Real Servers (RIPs)	11
Upload the Certificate	11
Configure SSL Termination	12
9.2. Application Servers	13
9.3. Finalizing the Configuration	13
10. Testing & Verification	13
10.1. Using System Overview	13
10.2. Access the Application	13
11. Technical Support	13
12. Further Documentation	13
13. Appendix	14
13.1. Configuring HA - Adding a Secondary Appliance	14
Non-Replicated Settings	14
Configuring the HA Clustered Pair	15
14. Document Revision History	17

1. About this Brief

This brief details the steps required to configure a load balanced Hyland OnBase environment utilizing Loadbalancer.org appliances. It covers the configuration of the load balancers and also any Hyland OnBase configuration changes that are required to enable load balancing.

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

2. Loadbalancer.org Appliances Supported

All our products can be used for load balancing Hyland OnBase. For full specifications of available models please refer to <https://www.loadbalancer.org/products>.

Some features may not be available or fully supported in all cloud platforms due to platform specific limitations. For more details, please refer to the "Main Differences to our Standard (Non-Cloud) Product" section in the appropriate cloud platform [Quick Start Guide](#) or check with Loadbalancer.org support.

3. Software Versions Supported

3.1. Loadbalancer.org Appliance

- V8.9.1 and later

Note

The screenshots used throughout this document aim to track the latest Loadbalancer.org software version. If you're using an older version, or the very latest, the screenshots presented here may not match your WebUI exactly.

3.2. Hyland OnBase

- All versions

4. Hyland OnBase

Hyland OnBase is a content services platform for managing content, processes and cases. It unites all your critical systems and information

5. Load Balancing Hyland OnBase

Note

It's highly recommended that you have a working Hyland OnBase environment first before implementing the load balancer.

5.1. Virtual Service (VIP) Requirements

To provide load balancing and HA for Hyland OnBase, multiple Web Servers and Application Servers are load balanced and the following VIPs are required:



Ref.	VIP Name	Use	Mode	Port(s)	Persistence Mode	Health Check
VIP 1	WebServers	Web Server traffic	L7 SNAT	80	HTTP Cookie	HTTP (GET)
VIP 2	AppServers	Application Server traffic	L7 SNAT	80	HTTP Cookie	HTTP (GET)

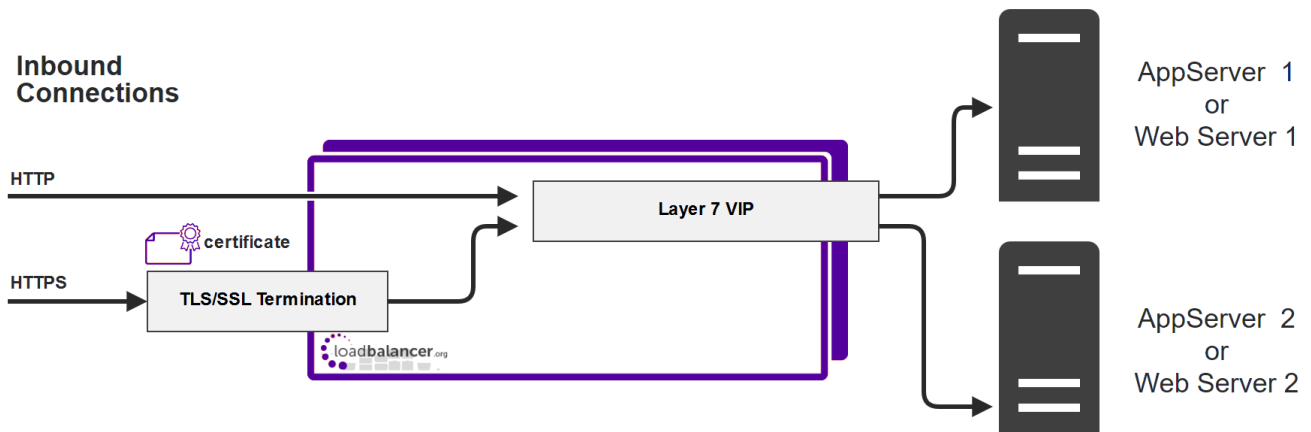
5.2. SSL Termination

SSL Termination is configured on the load balancer for the following VIPs:

- VIP 1 - **WebServers**
- VIP 2 - **AppServers**

This provides a corresponding HTTPS Virtual Service for these VIPs and allows HTTP persistence cookies to be inserted. Certificates in PEM or PFX format can be uploaded to the load balancer.

6. Deployment Concept



VIP = **V**irtual **I**P Address

Note

The load balancer can be deployed as a single unit, although Loadbalancer.org recommends a clustered pair for resilience & high availability. Please refer to [Configuring HA - Adding a Secondary Appliance](#) for more details on configuring a clustered pair.

7. Load Balancer Deployment Methods

The load balancer can be deployed in 4 fundamental ways: *Layer 4 DR mode*, *Layer 4 NAT mode*, *Layer 4 SNAT mode*, and *Layer 7 SNAT mode*.

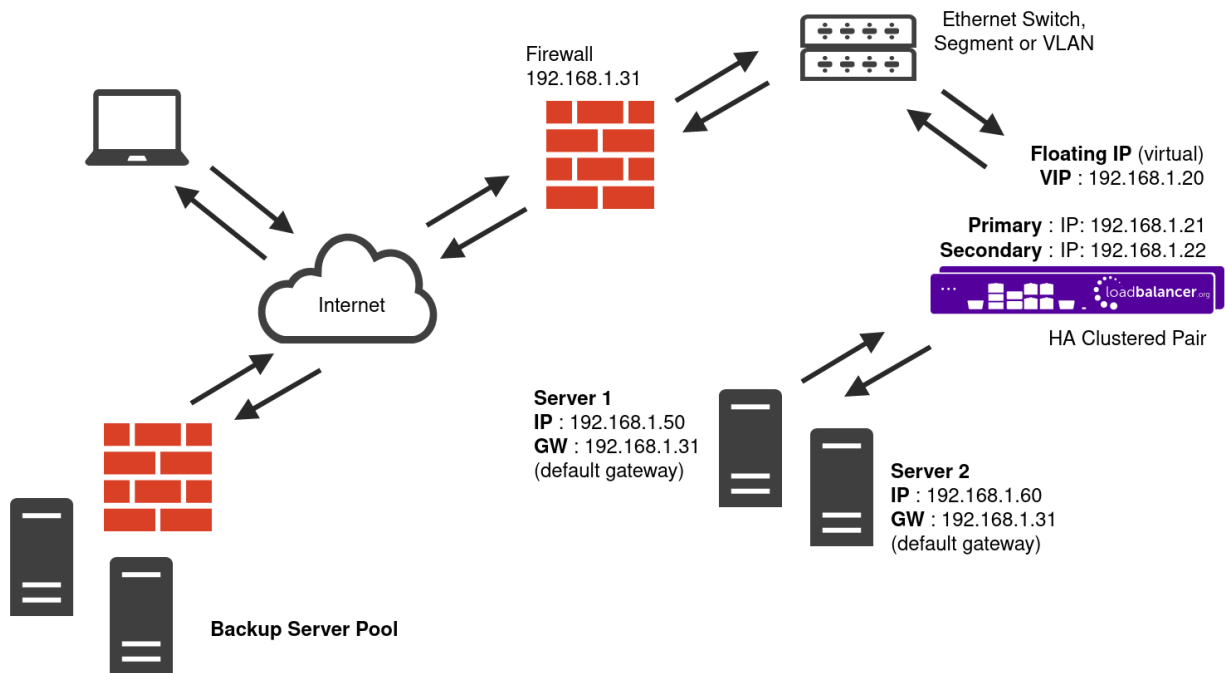
For Hyland OnBase, layer 7 SNAT mode is recommended. This mode is described below and is used for the configurations presented in this guide.

7.1. Layer 7 SNAT Mode

Layer 7 SNAT mode uses a proxy (HAProxy) at the application layer. Inbound requests are terminated on the load



balancer and HAProxy generates a new corresponding request to the chosen Real Server. As a result, Layer 7 is typically not as fast as the Layer 4 methods. Layer 7 is typically chosen when either enhanced options such as SSL termination, cookie based persistence, URL rewriting, header insertion/deletion etc. are required, or when the network topology prohibits the use of the layer 4 methods.



- Because layer 7 SNAT mode is a full proxy, any server in the cluster can be on any accessible subnet including across the Internet or WAN.
- Layer 7 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 balancer's 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. If required, the load balancer can be configured to provide the actual client IP address to the Real Servers in 2 ways. Either by inserting a header that contains the client's source IP address, or by modifying the Source Address field of the IP packets and replacing the IP address of the load balancer with the IP address of the client. For more information on these methods please refer to [Transparency at Layer 7](#).
- Layer 7 SNAT mode can be deployed using either a one-arm or two-arm configuration. For two-arm deployments, **eth0** is normally used for the internal network and **eth1** is used for the external network although this is not mandatory.
- Requires no mode-specific configuration changes to the load balanced Real Servers.
- Port translation is possible with Layer 7 SNAT mode, e.g. VIP:80 → RIP:8080 is supported.
- You should not use the same RIP:PORT combination for layer 7 SNAT mode VIPs and layer 4 SNAT mode VIPs because the required firewall rules conflict.

8. Loadbalancer.org Appliance – the Basics

8.1. Virtual Appliance

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, XEN and Nutanix AHV and has



been optimized for each Hypervisor. By default, the VA is allocated 2 vCPUs, 4GB of RAM and has a 20GB 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 [Virtual Appliance Installation](#) and the ReadMe.txt text file included in the VA download for additional information on deploying the VA using the various Hypervisors.

 **Note**

The VA has 4 network adapters. For VMware only the first adapter (**eth0**) is connected by default. For HyperV, KVM, XEN and Nutanix AHV all adapters are disconnected by default. Use the network configuration screen within the Hypervisor to connect the required adapters.

8.2. Initial Network Configuration

After boot up, follow the instructions on the appliance console to configure the management IP address, subnet mask, default gateway, DNS servers and other network and administrative settings.

 **Important**

Be sure to set a secure password for the load balancer, when prompted during the setup routine.

8.3. Accessing the Appliance WebUI

The WebUI is accessed using a web browser. By default, users are authenticated using Apache authentication. Users can also be authenticated against LDAP, LDAPS, Active Directory or Radius - for more information, please refer to [External Authentication](#).

 **Note**

There are certain differences when accessing the WebUI for the cloud appliances. For details, please refer to the relevant [Quick Start / Configuration Guide](#).

1. Using a browser, navigate to the following URL:

<https://<IP-address-configured-during-the-network-setup-wizard>:9443/lbadmin/>

 **Note**

You'll receive a warning about the WebUI's SSL certificate. This is due to the default self signed certificate that is used. If preferred, you can upload your own certificate - for more information, please refer to [Appliance Security Features](#).

 **Note**

If you need to change the port, IP address or protocol that the WebUI listens on, please refer to [Service Socket Addresses](#).

2. Log in to the WebUI using the following credentials:

Username: loadbalancer



Password: <configured-during-network-setup-wizard>

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

Once logged in, the WebUI will be displayed as shown below:

- You'll be asked if you want to run the Setup Wizard which can be used to configure layer 7 services. Click **Dismiss** if you're following a guide or want to configure the appliance manually or click **Accept** to start the wizard.

Main Menu Options

System Overview - Displays a graphical summary of all VIPs, RIPs and key appliance statistics

Local Configuration - Configure local host settings such as IP address, DNS, system time etc.

Cluster Configuration - Configure load balanced services such as VIPs & RIPs



Maintenance - Perform maintenance tasks such as service restarts and taking backups

View Configuration - Display the saved appliance configuration settings

Reports - View various appliance reports & graphs

Logs - View various appliance logs

Support - Create a support download, contact the support team & access useful links

Live Chat - Start a live chat session with one of our Support Engineers

8.4. Appliance Software Update

To ensure that the appliance(s) are running the latest software version, we recommend a software update check is performed.

Determining the Current Software Version

The software version is displayed at the bottom of the WebUI as shown in the example below:

Copyright © Loadbalancer.org Inc. 2002 – 2024
ENTERPRISE VA Max - v8.11.1

English ▼

Checking for Updates using Online Update

Note

By default, the appliance periodically contacts the Loadbalancer.org update server and checks for updates. An update check can also be manually triggered as detailed below.

1. Using the WebUI, navigate to: **Maintenance > Software Update**.
2. Select **Online Update**.
3. If the latest version is already installed, a message similar to the following will be displayed:

Information: Version v8.11.1 is the current release. No updates are available

4. If an update is available, you'll be presented with a list of new features, improvements, bug fixes and security related updates.
5. Click **Online Update** to start the update process.

Note

Do not navigate away whilst the update is ongoing, this may cause the update to fail.

6. Once complete (the update can take several minutes depending on download speed and upgrade version) the following message will be displayed:

Information: Update completed successfully.



7. If services need to be reloaded/restarted or the appliance needs a full restart, you'll be prompted accordingly.

Using Offline Update

If the load balancer does not have access to the Internet, offline update can be used.

Note

Please contact support@loadbalancer.org to check if an update is available and obtain the latest offline update files.

To perform an offline update:

1. Using the WebUI, navigate to: **Maintenance > Software Update**.
2. Select **Offline Update**.
3. The following screen will be displayed:

Software Update

Offline Update

The following steps will lead you through offline update.

1. Contact **Loadbalancer.org support** to obtain the offline update archive and checksum.
2. Save the archive and checksum to your local machine.
3. Select the archive and checksum files in the upload form below.
4. Click *Upload and Install* to begin the update process.

Archive: No file chosen

Checksum: No file chosen

4. Select the *Archive* and *Checksum* files.
5. Click **Upload and Install**.
6. If services need to be reloaded/restarted or the appliance needs a full restart, you'll be prompted accordingly.

8.5. Ports Used by the Appliance

By default, the appliance uses the following TCP & UDP ports:

Protocol	Port	Purpose
TCP	22 *	SSH
TCP & UDP	53 *	DNS / GSLB
TCP & UDP	123	NTP
TCP & UDP	161 *	SNMP
UDP	6694	Heartbeat between Primary & Secondary appliances in HA mode



Protocol	Port	Purpose
TCP	7778	HAProxy persistence table replication
TCP	9000 *	Gateway service (Centralized/Portal Management)
TCP	9080 *	WebUI - HTTP (disabled by default)
TCP	9081 *	Nginx fallback page
TCP	9443 *	WebUI - HTTPS
TCP	25565 *	Shuttle service (Centralized/Portal Management)

 **Note**

The ports used for SSH, GSLB, SNMP, the WebUI, the fallback page, the gateway service and the shuttle service can be changed if required. For more information, please refer to [Service Socket Addresses](#).

8.6. HA Clustered Pair Configuration

Loadbalancer.org recommend that load balancer appliances are deployed in pairs for high availability. In this Brief a single unit is deployed first, adding a secondary unit is covered in [Configuring HA - Adding a Secondary Appliance](#).

9. Appliance Configuration for Hyland OnBase

9.1. VIP 1 – WebServers

Virtual Service Configuration

- Using the WebUI, navigate to *Cluster Configuration > Layer 7 – Virtual Services* and click on **Add a new Virtual Service**.

Layer 7 - Add a new Virtual Service

Virtual Service
[Advanced +]

Label

WebServers

?

IP Address

192.168.10.100

?

Ports

80

?

Protocol

Layer 7 Protocol

HTTP Mode ▾

?

Cancel
Update

- Enter an appropriate *Label* (name) for the VIP, e.g. **WebServers**.
- Set the *Virtual Service IP* address field to the required IP address, e.g. **192.168.10.100**.



- Set the *Virtual Service Ports* field to **80**.
- Set the *Layer 7 Protocol* to **HTTP Mode**.
- Click **Update** to create the virtual service.
- Now click **Modify** next to the newly created VIP.
- Under *Persistence*, click **[Advanced]** to show more options.
- Ensure *Persistence Mode* is set to **HTTP Cookie**.
- Set *Cookie Max Idle Duration* to **60m** (60 minutes).
- Under *Health Checks*, set the *Health Check* to **Negotiate HTTP (GET)**.
- Leave *Request to Send* and *Response Expected* blank. This checks the root of the server, if a 2xx or 3xx response is received, the server is considered healthy.
- Under *Other*, click **[Advanced]** to show more options.
- Enable (check) the *Timeout* checkbox and set the *Client Timeout* and *Server Timeout* to **30m**.
- Click **Update**.

Define the Associated Real Servers (RIPs)

- Using WebUI, navigate to *Cluster Configuration > Layer 7 – Real Servers* and click on **Add a new Real Server** next to the newly created WebServers VIP.

Layer 7 Add a new Real Server

Label	<input type="text" value="Web1"/>	?
Real Server IP Address	<input type="text" value="192.168.10.120"/>	?
Real Server Port	<input type="text" value="80"/>	?
Re-Encrypt to Backend	<input type="checkbox"/>	?
Enable Redirect	<input type="checkbox"/>	?
Weight	<input type="text" value="100"/>	?

- Enter an appropriate *Label* for the server, e.g. **Web1**.
- Change the *Real Server IP Address* field to the required IP address, e.g. **192.168.10.120**.
- Set the *Real Server Port* field to **80**.
- Click **Update**.
- Repeat these steps to add additional Web servers as required.

Upload the Certificate



Note

A certificate in either PEM or PFX format can be uploaded to the load balancer.

1. Using the WebUI, navigate to: *Cluster Configuration* > *SSL Certificates*.
2. Click **Add a new SSL Certificate** and select *Upload prepared PEM/PFX file*.

I would like to:

- Upload prepared PEM/PFX file
- Create a new SSL Certificate Signing Request (CSR)
- Create a new Self-Signed SSL Certificate.

Label:

File to upload: No file chosen

3. Enter a suitable *Label* for the certificate, e.g. **Cert1**.
4. Browse to and select the certificate file to upload (PEM or PFX format).
5. Enter the password if applicable.
6. Click **Upload Certificate**.

Configure SSL Termination

1. Using the WebUI, navigate to: *Cluster Configuration* > *SSL Termination* and click **Add a new Virtual Service**.

Label:

Associated Virtual Service:

Virtual Service Port:

SSL Operation Mode:

SSL Certificate:

Source IP Address:

Enable Proxy Protocol:

Bind Proxy Protocol to L7 VIP:

2. Set the *Associated Virtual Service* to the appropriate VIP, e.g. **WebServers**.

Note

Once the VIP is selected, the Label field will be auto-populated with **SSL-WebServers**. This



can be changed if preferred.

3. Leave *Virtual Service Port* set to **443**.
4. Leave *SSL operation Mode* set to **High Security**.
5. Select the required certificate from the *SSL Certificate* drop-down, e.g. **Cert1**.
6. Click **Update**.

9.2. Application Servers

Repeat the steps in [Web Servers](#) to configure the load balancer for the Application Servers. Change IPs and names as required.

9.3. Finalizing the Configuration

To apply the new settings, HAProxy and STunnel must both be reloaded. This can be done using the buttons in the "Commit changes" box at the top of the screen or by using the **Restart Services** menu option:

1. Using the WebUI, navigate to: **Maintenance > Restart Services**.
2. Click **Reload HAProxy**.
3. Click **Reload STunnel**.

10. Testing & Verification

Note

For additional guidance on diagnosing and resolving any issues you may have, please also refer to [Diagnostics & Troubleshooting](#).

10.1. Using System Overview

The System Overview can be viewed in the WebUI. It shows a graphical view of all VIPs & RIPs (i.e. the Hyland OnBase servers) and shows the state/health of each server as well as the state of the cluster as a whole. This can be used to ensure all servers are up and available.

10.2. Access the Application

First ensure that any DNS records that are used to access the application are updated so they resolve to the relevant VIP. Then verify that you're able to successfully access the application.

11. 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.

12. Further Documentation

For additional information, please refer to the [Administration Manual](#).



13. Appendix

13.1. Configuring HA - Adding a Secondary Appliance

Our recommended configuration is to use a clustered HA pair of load balancers to provide a highly available and resilient load balancing solution. We recommend that the Primary appliance is fully configured first, then the Secondary appliance can be added to create an HA pair. Once the HA pair is configured, load balanced services must be configured and modified on the Primary appliance. The Secondary appliance will be automatically kept in sync.

 **Note**

For Enterprise Azure, the HA pair should be configured first. For more information, please refer to the Azure Quick Start/Configuration Guide available in the [documentation library](#)

The clustered HA pair uses Heartbeat to determine the state of the other appliance. Should the active device (normally the Primary) suffer a failure, the passive device (normally the Secondary) will take over.

Non-Replicated Settings

A number of settings are not replicated as part of the Primary/Secondary pairing process and therefore must be manually configured on the Secondary appliance. These are listed by WebUI menu option in the table below:

WebUI Main Menu Option	Sub Menu Option	Description
Local Configuration	Hostname & DNS	Hostname and DNS settings
Local Configuration	Network Interface Configuration	Interface IP addresses, bonding configuration and VLANs
Local Configuration	Routing	Default gateways and static routes
Local Configuration	System Date & time	Time and date related settings
Local Configuration	Physical – Advanced Configuration	Various appliance settings
Local Configuration	Portal Management	Portal management settings
Local Configuration	Security	Security settings
Local Configuration	SNMP Configuration	SNMP settings
Local Configuration	Graphing	Graphing settings
Local Configuration	License Key	Appliance licensing
Maintenance	Backup & Restore	Local XML backups
Maintenance	Software Updates	Appliance software updates
Maintenance	Fallback Page	Fallback page configuration
Maintenance	Firewall Script	Firewall (iptables) configuration
Maintenance	Firewall Lockdown Wizard	Appliance management lockdown settings

⚠ Important

Make sure that where any of the above have been configured on the Primary appliance, they're also configured on the Secondary.

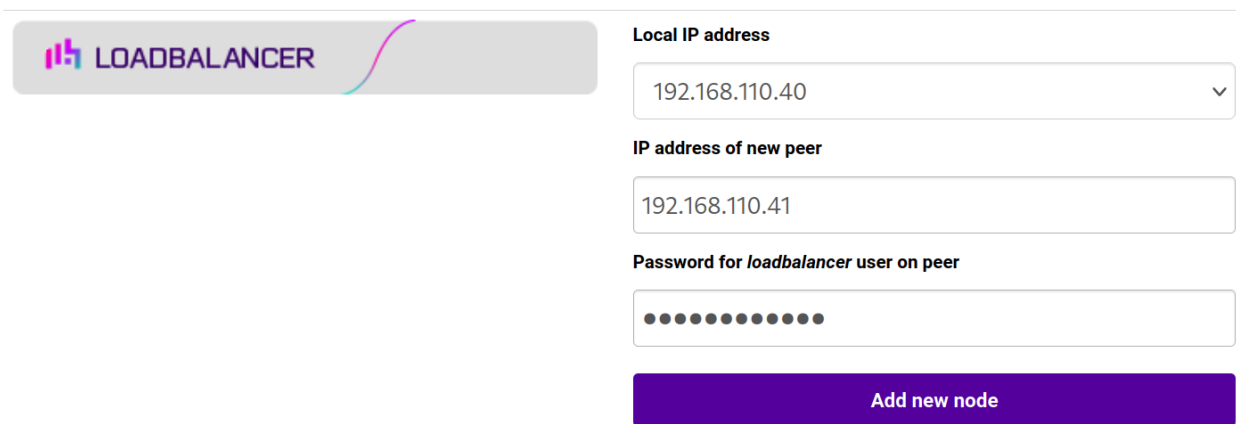
Configuring the HA Clustered Pair

📌 Note

If you have already run the firewall lockdown wizard on either appliance, you'll need to ensure that it is temporarily disabled on both appliances whilst performing the pairing process.

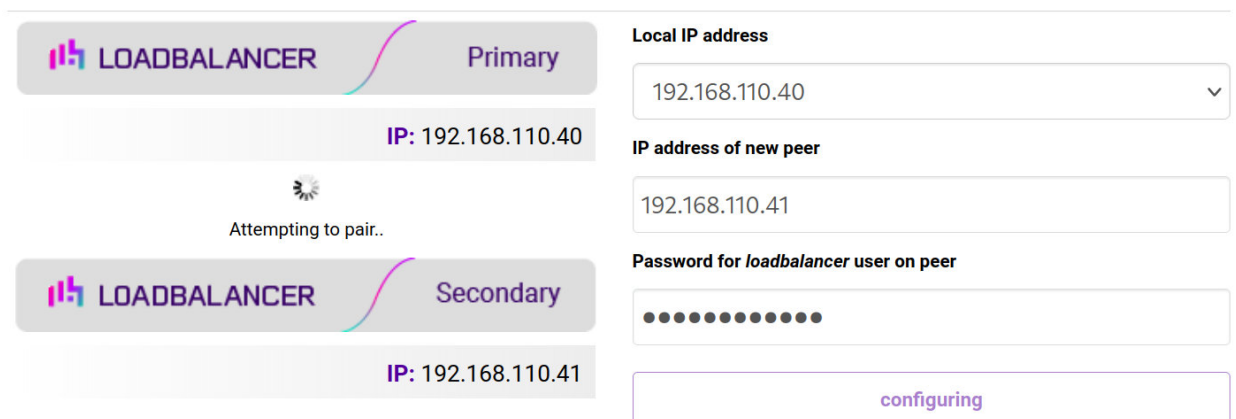
1. Deploy a second appliance that will be the Secondary and configure initial network settings.
2. Using the WebUI on the Primary appliance, navigate to: *Cluster Configuration > High-Availability Configuration*.

Create a Clustered Pair



3. Specify the IP address and the *loadbalancer* user's password for the Secondary (peer) appliance as shown in the example above.
4. Click **Add new node**.
5. The pairing process now commences as shown below:

Create a Clustered Pair



6. Once complete, the following will be displayed on the Primary appliance:

High Availability Configuration - primary

The screenshot displays a configuration interface for a High Availability (HA) setup. It features two load balancer appliances, each represented by a grey rounded rectangle with a purple icon and a pink-to-purple gradient line. The top appliance is labeled 'LOADBALANCER Primary' and has the IP address 'IP: 192.168.110.40'. The bottom appliance is labeled 'LOADBALANCER Secondary' and has the IP address 'IP: 192.168.110.41'. To the right of these appliances is a prominent red button with the text 'Break Clustered Pair'.

7. To finalize the configuration, restart heartbeat and any other services as prompted in the "Commit changes" message box at the top of the screen.

Note

Clicking the **Restart Heartbeat** button on the Primary appliance will also automatically restart heartbeat on the Secondary appliance.

Note

For more details on configuring HA with 2 appliances, please refer to [Appliance Clustering for HA](#).

Note

For details on testing and verifying HA, please refer to [Clustered Pair Diagnostics](#).

14. Document Revision History

Version	Date	Change	Reason for Change	Changed By
1.1.0	9 September 2019	Styling and layout	General styling updates	AH
1.1.1	28 August 2020	New title page Updated Canadian contact details Amended instructions for setting persistence and timeout options	Branding update Change to Canadian contact details Changes to the appliance WebUI	AH
1.2.0	1 December 2021	Converted the document to AsciiDoc	Move to new documentation system	AH, RJC, ZAC
1.2.1	22 April 2022	Updated SSL related content to reflect latest software version	New software release	RJC
1.2.2	28 September 2022	Updated layer 7 VIP and RIP creation screenshots	Reflect changes in the web user interface	AH
1.2.3	5 January 2023	Combined software version information into one section Added one level of section numbering Added software update instructions Added table of ports used by the appliance Reworded 'Further Documentation' section Removed references to the colour of certain UI elements	Housekeeping across all documentation	AH
1.2.4	2 February 2023	Updated screenshots	Branding update	AH
1.2.5	7 March 2023	Removed conclusion section	Updates across all documentation	AH
1.3.0	24 March 2023	New document theme Modified diagram colours	Branding update	AH

Version	Date	Change	Reason for Change	Changed By
1.4.0	30 April 2024	Restructured document to follow standard format Re-classified as a "Brief" Various updates and corrections	Required updates	RJC





Visit us: www.loadbalancer.org

Phone us: +44 (0)330 380 1064

Phone us: +1 833 274 2566

Email us: info@loadbalancer.org

Follow us: [@loadbalancer.org](https://twitter.com/loadbalancer.org)

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.

