

Load Balancing Epic EHR

Version 1.1.0



Table of Contents

1. About this Guide	3
2. Loadbalancer.org Appliances Supported	3
3. Software Versions Supported	3
3.1. Loadbalancer.org Appliance	3
3.2. Epic EHR	3
4. Epic EHR	3
5. Load Balancing Epic EHR	3
5.1. Persistence (aka Server Affinity)	4
5.2. Virtual Service (VIP) Requirements	4
5.3. Port Requirements	4
6. Deployment Concept	4
7. Loadbalancer.org Appliance – the Basics	5
7.1. Virtual Appliance	5
7.2. Initial Network Configuration	5
7.3. Accessing the Appliance WebUI	5
Main Menu Options	7
7.4. Appliance Software Update	7
Determining the Current Software Version	7
Checking for Updates using Online Update	7
Using Offline Update	8
7.5. Ports Used by the Appliance	8
7.6. HA Clustered Pair Configuration	9
8. Appliance Configuration for Epic EHR	9
8.1. Configuring VIP 1 – Hyperspace	9
Configuring the Virtual Service (VIP)	9
Defining the Real Servers (RIPs)	10
8.2. Configuring VIP 2 – Hyperspace Redirect	10
Configuring the Virtual Service (VIP)	11
8.3. Configuring VIP 3 – MyChart (Optional)	11
Configuring the Virtual Service (VIP)	11
Defining the Real Servers (RIPs)	12
8.4. Configuring VIP 4 – MyChart Redirect (Optional)	12
Configuring the Virtual Service (VIP)	13
8.5. Finalizing the Configuration	13
9. Testing & Verification	14
9.1. Using System Overview	14
10. Technical Support	14
11. Further Documentation	14
12. Appendix	15
12.1. Configuring HA - Adding a Secondary Appliance	15
Non-Replicated Settings	15
Adding a Secondary Appliance - Create an HA Clustered Pair	16
13. Document Revision History	18

1. About this Guide

This guide details the steps required to configure a load balanced Epic EHR environment utilizing Loadbalancer.org appliances. It covers the configuration of the load balancers and also any Epic EHR 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 with Epic EHR. For full specifications of available models please refer to <https://www.loadbalancer.org/products>.

Some features may not be supported in all cloud platforms due to platform specific limitations, please check with Loadbalancer.org support for further details.

3. Software Versions Supported

3.1. Loadbalancer.org Appliance

- V8.6.1 and later

Note

The screenshots used throughout this document aim to track the latest Loadbalancer.org software version. If using an older software version, note that the screenshots presented here may not match the WebUI exactly.

3.2. Epic EHR

- All versions

4. Epic EHR

The Epic EHR (Electronic Health Records) software suite brings together essential tools for clinicians and patients in the healthcare space.

Epic Hyperspace is a clinician-facing platform. It's a front-end client used to access most parts of the Epic software suite, including patient charts, prescribing, and even print services.

Epic MyChart is a patient-facing web portal. It gives patients the ability to view their medical records and test results, manage their appointments and prescriptions, and more.

5. Load Balancing Epic EHR

Note

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



5.1. Persistence (aka Server Affinity)

The Epic EHR applications require sessions to stick to the same real server. Source IP address affinity is used to achieve this.

5.2. Virtual Service (VIP) Requirements

To provide load balancing and HA for Epic EHR, the following VIPs are required:

- Hyperspace
- Hyperspace redirect (to force inbound HTTP traffic to use HTTPS)

Optionally, additional VIPs may be required as follows:

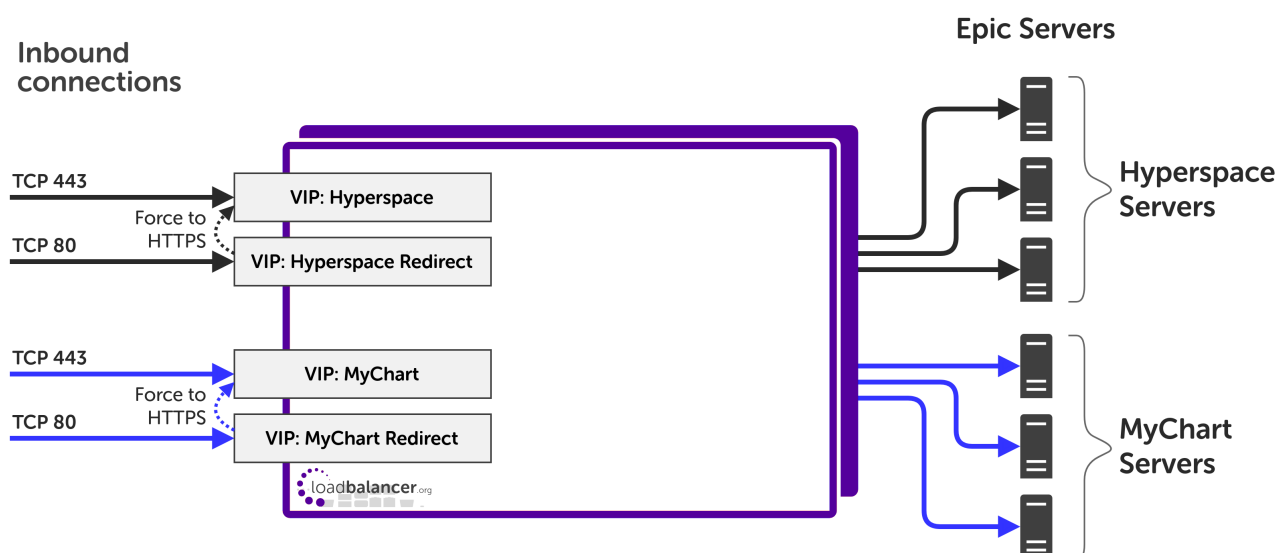
- MyChart
- MyChart redirect (to force inbound HTTP traffic to use HTTPS)

5.3. Port Requirements

The following table shows the ports that are load balanced:

Port	Protocols	Use
80	TCP/HTTP	Redirect to HTTPS (not strictly load balanced)
443	TCP/HTTPS	Web Services

6. Deployment Concept



VIPs = Virtual IP Addresses

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 the section [Configuring HA](#) -



7. Loadbalancer.org Appliance – the Basics

7.1. 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.

7.2. Initial Network Configuration

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

Important

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

7.3. 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](#).

Note

A number of compatibility issues have been found with various versions of Microsoft Internet Explorer and Edge. The WebUI has been tested and verified using both Chrome & Firefox.

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 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](#).

- Log in to the WebUI using the following credentials:

Username: loadbalancer

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



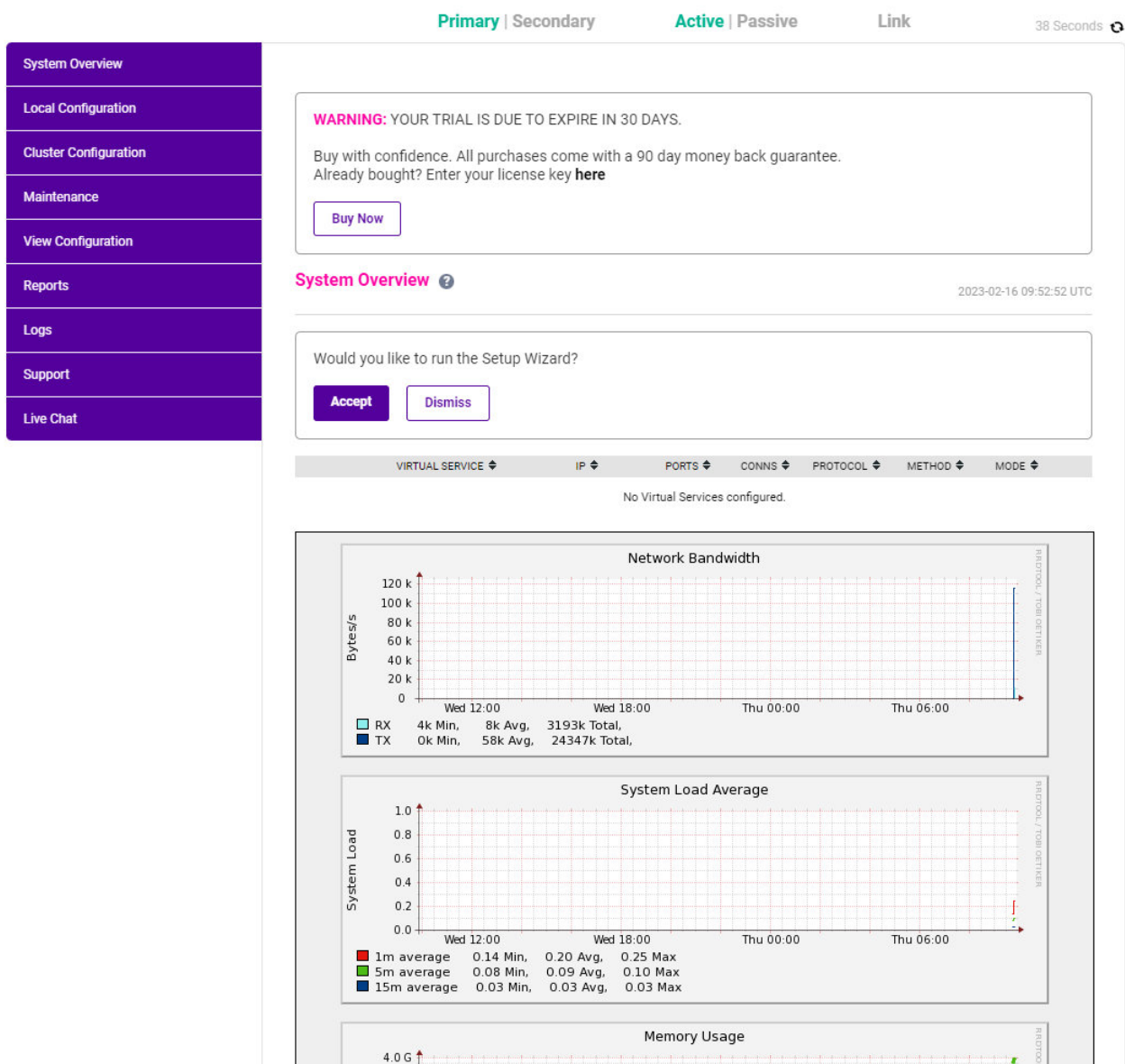
Note

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

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

 **LOADBALANCER**

Enterprise VA Max



3. You'll be asked if you want to run the Setup Wizard. Click **Dismiss** if you're following a guide or want to configure the appliance manually. Click **Accept** to start the Setup Wizard.



Note

The Setup Wizard can only be used to configure Layer 7 services.

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

7.4. 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 – 2023
ENTERPRISE VA Max - v8.9.0

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 v8.9.0 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.



- 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.

- 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.

- 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:

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

Software Update

Offline Update

The following steps will lead you through offline update.

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

Archive: No file chosen

Checksum: No file chosen

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

7.5. 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
TCP & UDP	123	NTP
TCP & UDP	161	SNMP
UDP	6694	Heartbeat between Primary & Secondary appliances in HA mode
TCP	7778	HAProxy persistence table replication
TCP	9080	WebUI - HTTP (disabled by default)
TCP	9081	Nginx fallback page
TCP	9443	WebUI - HTTPS

7.6. 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 unit is covered in the section [Configuring HA - Adding a Secondary Appliance](#) of the appendix.

8. Appliance Configuration for Epic EHR

8.1. Configuring VIP 1 – Hyperspace

Configuring the Virtual Service (VIP)

1. Using the web user interface, navigate to *Cluster Configuration > Layer 7 – Virtual Services* and click on **Add a new Virtual Service**.
2. Define the *Label* for the virtual service as required, e.g. **Hyperspace**.
3. Set the *Virtual Service IP Address* field to the required IP address, e.g. **192.168.85.150**.
4. Set the *Ports* field to **443**.
5. Set the *Layer 7 Protocol* to **TCP Mode**.
6. Click **Update** to create the virtual service.

Layer 7 - Add a new Virtual Service

Virtual Service		[Advanced +]
Label	<input type="text" value="Hyperspace"/>	?
IP Address	<input type="text" value="192.168.85.150"/>	?
Ports	<input type="text" value="443"/>	?
Protocol		
Layer 7 Protocol	<input type="text" value="TCP Mode"/>	?

- Click **Modify** next to the newly created VIP.
- In the **Persistence** section click **Advanced** to expand the menu.
- Set **Timeout** to **60** (the default units are minutes).
- Click **Update**.

Persistence		[Advanced]
Persistence Mode	<input type="text" value="Source IP"/>	?
Persistence	Timeout <input type="text" value="60"/>	?

Defining the Real Servers (RIPs)

- Using the web user interface, navigate to **Cluster Configuration > Layer 7 – Real Servers** and click on **Add a new Real Server** next to the newly created VIP.
- Define the **Label** for the real server as required, e.g. **Hyperspace_Srv_1**.
- Set the **Real Server IP Address** field to the required IP address, e.g. **192.168.85.200**.
- Click **Update**.
- Repeat these steps to add additional servers as required.

Layer 7 Add a new Real Server - Hyperspace

Label	<input type="text" value="Hyperspace_Srv_1"/>	?
Real Server IP Address	<input type="text" value="192.168.85.200"/>	?
Real Server Port	<input type="text"/>	?
Re-Encrypt to Backend	<input type="checkbox"/>	?
Weight	<input type="text" value="100"/>	?

8.2. Configuring VIP 2 – Hyperspace Redirect

Configuring the Virtual Service (VIP)

1. Using the web user interface, navigate to *Cluster Configuration > Layer 7 – Virtual Services* and click on **Add a new Virtual Service**.
2. Define the **Label** for the virtual service as required, e.g. **Hyperspace_redirect**.
3. Set the **Virtual Service IP Address** field to the **same** IP address used for the Hyperspace VIP, e.g. **192.168.85.150**.
4. Set the **Ports** field to **80**.
5. Set the **Layer 7 Protocol** to **HTTP Mode**.
6. Click **Update** to create the virtual service.

Layer 7 - Add a new Virtual Service

Virtual Service		[Advanced +]
Label	<input type="text" value="Hyperspace_redirect"/>	?
IP Address	<input type="text" value="192.168.85.150"/>	?
Ports	<input type="text" value="80"/>	?
Protocol		
Layer 7 Protocol	<input type="text" value="HTTP Mode"/>	?

7. Click **Modify** next to the newly created VIP.
8. In the **Other** section click **Advanced** to expand the menu.
9. Set **Force to HTTPS** to **Yes**.
10. Click **Update**.

Force to HTTPS

☒ Yes ☐ No

8.3. Configuring VIP 3 – MyChart (Optional)

Configuring the Virtual Service (VIP)

1. Using the web user interface, navigate to *Cluster Configuration > Layer 7 – Virtual Services* and click on **Add a new Virtual Service**.
2. Define the **Label** for the virtual service as required, e.g. **MyChart**.
3. Set the **Virtual Service IP Address** field to the required IP address, e.g. **192.168.85.151**.
4. Set the **Ports** field to **443**.
5. Set the **Layer 7 Protocol** to **TCP Mode**.
6. Click **Update** to create the virtual service.



Layer 7 - Add a new Virtual Service

Virtual Service		[Advanced +]
Label	<input type="text" value="MyChart"/>	?
IP Address	<input type="text" value="192.168.85.151"/>	?
Ports	<input type="text" value="443"/>	?
Protocol		
Layer 7 Protocol	<input type="text" value="TCP Mode"/>	?

- Click **Modify** next to the newly created VIP.
- In the **Persistence** section click **Advanced** to expand the menu.
- Set **Timeout** to **60** (the default units are minutes).
- Click **Update**.

Persistence		[Advanced]
Persistence Mode	<input type="text" value="Source IP"/>	?
Persistence	Timeout <input type="text" value="60"/>	?

Defining the Real Servers (RIPs)

- Using the web user interface, navigate to **Cluster Configuration > Layer 7 – Real Servers** and click on **Add a new Real Server** next to the newly created VIP.
- Define the **Label** for the real server as required, e.g. **MyChart_Srv_1**.
- Set the **Real Server IP Address** field to the required IP address, e.g. **192.168.85.210**.
- Click **Update**.
- Repeat these steps to add additional servers as required.

Layer 7 Add a new Real Server - MyChart

Label	<input type="text" value="MyChart_Srv_1"/>	?
Real Server IP Address	<input type="text" value="192.168.85.210"/>	?
Real Server Port	<input type="text"/>	?
Re-Encrypt to Backend	<input type="checkbox"/>	?
Weight	<input type="text" value="100"/>	?

8.4. Configuring VIP 4 – MyChart Redirect (Optional)



Note

If the optional **MyChart** VIP has been configured then this redirect VIP must also be configured to ensure proper operation of the load balanced MyChart service.

Configuring the Virtual Service (VIP)

1. Using the web user interface, navigate to **Cluster Configuration > Layer 7 – Virtual Services** and click on **Add a new Virtual Service**.
2. Define the **Label** for the virtual service as required, e.g. **MyChart_redirect**.
3. Set the **Virtual Service IP Address** field to the **same** IP address used for the MyChart VIP, e.g. **192.168.85.151**.
4. Set the **Ports** field to **80**.
5. Set the **Layer 7 Protocol** to **HTTP Mode**.
6. Click **Update** to create the virtual service.

Layer 7 - Add a new Virtual Service

Virtual Service		[Advanced +]
Label	<input type="text" value="MyChart_redirect"/>	?
IP Address	<input type="text" value="192.168.85.151"/>	?
Ports	<input type="text" value="80"/>	?
Protocol		
Layer 7 Protocol	<input type="text" value="HTTP Mode"/>	?

7. Click **Modify** next to the newly created VIP.
8. In the **Other** section click **Advanced** to expand the menu.
9. Set **Force to HTTPS** to **Yes**.
10. Click **Update**.

Force to HTTPS

☒ Yes ☐ No

8.5. Finalizing the Configuration

To apply the new settings, HAProxy must be reloaded. This can be done using the button 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**.



9. Testing & Verification

Note

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

9.1. Using System Overview

The System Overview can be viewed in the WebUI. It shows a graphical view of all VIPs & RIPs (i.e. the Hyperspace and MyChart 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 all servers of both services are healthy and available to accept connections:

System Overview ?

2022-02-21 18:00:20 UTC

	VIRTUAL SERVICE	IP	PORTS	CONNS	PROTOCOL	METHOD	MODE	
↑	Hyperspace	192.168.85.150	443	0	TCP	Layer 7	Proxy	
	REAL SERVER	IP	PORTS	WEIGHT	CONNS			
↑	Hyperspace_Srv_1	192.168.85.200	443	100	0	Drain	Halt	
↑	Hyperspace_Srv_2	192.168.85.201	443	100	0	Drain	Halt	
↑	Hyperspace_Srv_3	192.168.85.202	443	100	0	Drain	Halt	
↑	Hyperspace_redir..	192.168.85.150	80	0	HTTP	Layer 7	Proxy	
↑	MyChart	192.168.85.151	443	0	TCP	Layer 7	Proxy	
	REAL SERVER	IP	PORTS	WEIGHT	CONNS			
↑	MyChart_Srv_1	192.168.85.210	443	100	0	Drain	Halt	
↑	MyChart_Srv_2	192.168.85.211	443	100	0	Drain	Halt	
↑	MyChart_redirect..	192.168.85.151	80	0	HTTP	Layer 7	Proxy	

10. 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.

11. Further Documentation

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



12. Appendix

12.1. 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 configured first and then the Secondary should be added. Once the Primary and Secondary are paired, all load balanced services configured on the Primary are automatically replicated to the Secondary over the network using SSH/SCP.

Note

For Enterprise Azure, the HA pair should be configured first. In Azure, when creating a VIP using an HA pair, 2 private IPs must be specified – one for the VIP when it's active on the Primary and one for the VIP when it's active on the Secondary. Configuring the HA pair first, enables both IPs to be specified when the VIP is created.

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	All network settings including IP address(es), bonding configuration and VLANs
Local Configuration	Routing	Routing configuration including default gateways and static routes
Local Configuration	System Date & time	All time and date related settings
Local Configuration	Physical – Advanced Configuration	Various settings including Internet Proxy, Management Gateway, Firewall connection tracking table size, NIC offloading, SMTP relay, logging and Syslog Server
Local Configuration	Security	Appliance security settings
Local Configuration	SNMP Configuration	Appliance SNMP settings
Local Configuration	Graphing	Appliance graphing settings
Local Configuration	License Key	Appliance licensing
Maintenance	Software Updates	Appliance software update management
Maintenance	Firewall Script	Appliance firewall (iptables) configuration
Maintenance	Firewall Lockdown Wizard	Appliance management lockdown settings

⚠ Important

Make sure that if these settings/updates have been configured on the Primary appliance, they're also configured on the Secondary appliance.


Adding a Secondary Appliance - Create an 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

 **LOADBALANCER**

Local IP address

192.168.110.40

IP address of new peer

192.168.110.41


Password for *loadbalancer* user on peer

••••••••••

Add new node

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

 **LOADBALANCER**

Primary

IP: 192.168.110.40

Attempting to pair..

 **LOADBALANCER**

Secondary

IP: 192.168.110.41

Local IP address

192.168.110.40

IP address of new peer

192.168.110.41

Password for *loadbalancer* user on peer





••••••••••

configuring

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



High Availability Configuration - primary

 LOADBALANCER  Primary	Break Clustered Pair
IP: 192.168.110.40	Make Active
 LOADBALANCER  Secondary	
IP: 192.168.110.41	

- 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](#).

13. Document Revision History

Version	Date	Change	Reason for Change	Changed By
1.0.0	22 February 2022	Initial version		AH
1.0.1	28 September 2022	Updated layer 7 VIP and RIP creation screenshots	Reflect changes in the web user interface	AH
1.0.2	5 January 2023	<p>Combined software version information into one section</p> <p>Added one level of section numbering</p> <p>Added software update instructions</p> <p>Added table of ports used by the appliance</p> <p>Reworded 'Further Documentation' section</p> <p>Removed references to the colour of certain UI elements</p>	Housekeeping across all documentation	AH
1.0.3	2 February 2023	Updated screenshots	Branding update	AH
1.0.4	7 March 2023	Removed conclusion section	Updates across all documentation	AH
1.1.0	24 March 2023	<p>New document theme</p> <p>Modified diagram colours</p>	Branding update	AH



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.

