

Load Balancing Philips IntelliSpace PACS

Version 1.3.0



Table of Contents

1. About this Guide	4
2. Loadbalancer.org Appliances Supported	4
3. Software Versions Supported	4
3.1. Loadbalancer.org Appliance	4
3.2. Philips IntelliSpace PACS	4
4. Philips IntelliSpace PACS	4
5. Load Balancing Philips IntelliSpace PACS	4
5.1. Persistence (aka Server Affinity)	5
5.2. Virtual Service (VIP) Requirements	5
5.3. Port Requirements	5
5.4. Health Checks	5
5.5. Specifying Traffic Source Address / SNAT Options	6
6. Deployment Concept	6
7. Loadbalancer.org Appliance – the Basics	6
7.1. Virtual Appliance	6
7.2. Initial Network Configuration	7
7.3. Accessing the Appliance WebUI	7
7.3.1. Main Menu Options	8
7.4. Appliance Software Update	9
7.4.1. Online Update	9
7.4.2. Offline Update	9
7.5. Ports Used by the Appliance	10
7.6. HA Clustered Pair Configuration	11
8. Appliance Configuration for Philips IntelliSpace PACS – Using Layer 7 SNAT Mode	11
8.1. Configuring the External Health Check Scripts	11
8.1.1. Ping Check	11
8.1.2. MS-SQL Check	11
8.2. Configuring VIP 1 – DICOM	12
8.2.1. Configuring the Virtual Service (VIP)	12
8.2.2. Defining the Real Servers (RIPs)	13
8.3. Configuring VIP 2 – DICOM Secure	13
8.3.1. Configuring the Virtual Service (VIP)	13
8.3.2. Defining the Real Servers (RIPs)	14
8.4. Configuring VIP 3 – DMWL	14
8.4.1. Configuring the Virtual Service (VIP)	14
8.4.2. Defining the Real Servers (RIPs)	15
8.5. Configuring VIP 4 – DMWL Secure	16
8.5.1. Configuring the Virtual Service (VIP)	16
8.5.2. Defining the Real Servers (RIPs)	17
8.6. Configuring VIP 5 – SQL	17
8.6.1. Configuring the Virtual Service (VIP)	17
8.6.2. Defining the Real Servers (RIPs)	18
8.7. Configuring VIP 6 – LDAP	19
8.7.1. Configuring the Virtual Service (VIP)	19
8.7.2. Defining the Real Servers (RIPs)	20
8.8. Configuring VIP 6 – LDAP Secure (LDAPS)	20
8.8.1. Configuring the Virtual Service (VIP)	20
8.8.2. Defining the Real Servers (RIPs)	21

8.9. Configuring VIP 7 – QRSCP	22
8.9.1. Configuring the Virtual Service (VIP)	22
8.9.2. Defining the Real Servers (RIPs)	22
8.10. Configuring VIP 8 – QRSCP Secure	23
8.10.1. Configuring the Virtual Service (VIP)	23
8.10.2. Defining the Real Servers (RIPs)	24
8.11. Finalizing the Configuration	24
9. Testing & Verification	24
9.1. Using System Overview	25
10. Technical Support	25
11. Further Documentation	25
12. Appendix	26
12.1. Configuring Outbound SNAT Rules for DICOM Services (iExport and iQuery)	26
12.1.1. Example SNAT rule	26
12.1.2. Example SNAT rule using multiple IP addresses	26
12.2. Source IP Transparency at Layer 7 Using TPROXY	26
12.3. Configuring HA - Adding a Secondary Appliance	27
12.3.1. Non-Replicated Settings	27
12.3.2. Configuring the HA Clustered Pair	28
13. Document Revision History	30

1. About this Guide

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

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. Philips IntelliSpace PACS

- All versions

4. Philips IntelliSpace PACS

Philips IntelliSpace PACS is an enterprise medical imaging solution and workflow. It gives clinicians rapid access to the images needed throughout the whole patient care cycle. It is based on open standards, allowing for interoperability with other systems.

The system processes and presents patient data in an intelligent way, combining data from multiple sources into a single comprehensive view for analysis. It is designed to be secure and to respect patient confidentiality through the appropriate handling of data.

5. Load Balancing Philips IntelliSpace PACS

 **Note**

It's highly recommended that you have a working Philips IntelliSpace PACS environment first before implementing the load balancer.



5.1. Persistence (aka Server Affinity)

Source IP address persistence is used for every virtual service involved in load balancing Philips IntelliSpace PACS. This ensures that a client connects to the same back end real server for their entire session.

5.2. Virtual Service (VIP) Requirements

To provide load balancing and HA for Philips IntelliSpace PACS, the following VIPs are required:

- DICOM
- DICOM Secure
- DMWL
- DMWL Secure
- SQL
- LDAP
- LDAP Secure
- QRSCP
- QRSCP Secure

5.3. Port Requirements

The following table shows the ports that are load balanced:

Port	Protocols	Use
104	TCP/DICOM	DICOM traffic
2762	TCP/TLS/DICOM	DICOM traffic over TLS, "DICOM secure"
8104	TCP/DICOM	DMWL traffic (DICOM Modality Worklists) traffic
10104	TCP/TLS/DICOM	DMWL traffic over TLS, "DMWL secure"
1433	TCP/SQL	MS SQL service
3890	TCP/LDAP	LDAP service
6360	TCP/LDAPS	Secure LDAP service
107	TCP/DICOM	QRSCP service (Query/Retrieve Service Class Provider)
2765	TCP/TLS/DICOM	QRSCP service over TLS, "QRSCP secure"

5.4. Health Checks

Load balancing a Philips IntelliSpace deployment requires using three different health checks.

Most virtual services use the default **Connect to port** health check. The exceptions are the DMWL and QRSCP virtual services, which use ping based checks, and the SQL virtual service, which uses a proprietary MS SQL health check.



The Microsoft SQL health check requires the Microsoft ODBC Driver. Because it is not free and open source software, this driver cannot be redistributed with our load balancer.

We have a blog post on our website which walks through how to set up and use this health check. This blog post is available here: <https://www.loadbalancer.org/blog/ms-sql-health-check/>

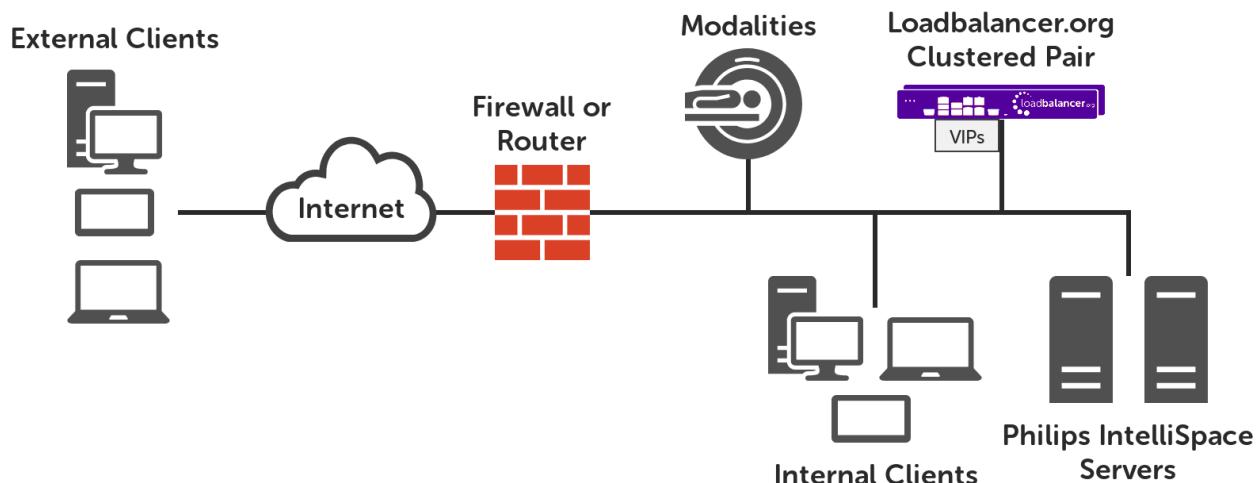
5.5. Specifying Traffic Source Address / SNAT Options

This guide contains references to using the **Set Source Address** option. This option may be required to successfully implement load balancing in a Philips IntelliSpace deployment.

For a given virtual service, the **Set Source Address** option makes outgoing traffic leave the load balancer from a specified IP address that it owns. When using a pair of load balancers, an IP address specified in this way should be a floating IP address so that it can "float" between and function correctly on either appliance when active. Such an address can be defined through the WebUI under *Cluster Configuration > Floating IPs*.

Using the **Set Source Address** option is useful when the back end real servers that the load balancer is querying require incoming traffic to originate from a specific, possibly trusted or whitelisted, IP address.

6. Deployment Concept



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. 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](#).



i 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.

i 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.

i 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 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.

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](#).

i 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/>

i 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](#).

i 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>





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**

Primary | Secondary Active | Passive Link 8 Seconds

System Overview

WARNING: YOUR TRIAL IS DUE TO EXPIRE IN 30 DAYS.
Buy with confidence. All purchases come with a 90 day money back guarantee.
Already bought? Enter your license key [here](#)

Buy Now

System Overview 2025-05-08 12:37:21 UTC

Would you like to run the Setup Wizard?

Accept **Dismiss**

VIRTUAL SERVICE **IP** **PORTS** **CONN** **PROTOCOL** **METHOD** **MODE**

No Virtual Services configured.

Network Bandwidth

Bytes/s

200 k, 150 k, 100 k, 50 k, 0

2025-05-08 12:37:21 UTC

Wed 18:00, Thu 00:00, Thu 06:00, Thu 12:00

RX 28 Min, 2713 Avg, 27344772 Total, **TX** 0 Min, 13777 Avg, 138872181 Total,

System Load Average

System Load

1.0, 0.8, 0.6, 0.4, 0.2, 0.0

2025-05-08 12:37:21 UTC

Wed 18:00, Thu 00:00, Thu 06:00, Thu 12:00

1m average 0.00 Min, 0.08 Avg, 0.68 Max
5m average 0.00 Min, 0.04 Avg, 0.30 Max
15m average 0.00 Min, 0.02 Avg, 0.12 Max

Memory Usage

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.



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

7.3.1. Main Menu Options

System Overview - Displays a graphical summary of all VIPs, RIPv2 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 & RIPv2



Maintenance - Perform maintenance tasks such as service restarts and creating 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

We recommend that the appliance is kept up to date to ensure that you benefit from the latest bug fixes, security updates and feature improvements. Both online and offline update are supported.

 **Note**

For full details, please refer to [Appliance Software Update](#) in the Administration Manual.

 **Note**

Services may need to be restarted/reloaded after the update process completes or in some cases a full appliance restart may be required. We therefore recommend performing the update during a maintenance window.

7.4.1. Online Update

The appliance periodically contacts the Loadbalancer.org update server (**update.loadbalancer.org**) and checks for updates. This is the default behavior and can be disabled if preferred. If an update is found, a notification similar to the example below will be displayed at the top of the WebUI:

Information: Update 8.13.2 is now available for this appliance.

Online Update

Click **Online Update**. A summary of all new features, improvements, bug fixes and security updates included in the update will be displayed. Click **Update** at the bottom of the page to start the update process.

 **(!) Important**

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

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

Information: Update completed successfully. Return to system overview.

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

7.4.2. Offline Update

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



To check for the latest version, please refer to our product roadmap page available [here](#). To obtain the latest offline update files contact support@loadbalancer.org.

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.

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 / GSLB
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	9000 *	Gateway service (Centralized/Portal Management)
TCP	9080 *	WebUI - HTTP (disabled by default)
TCP	9081 *	Nginx fallback page
TCP	9443 *	WebUI - HTTPS



Protocol	Port	Purpose
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](#).

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 [Configuring HA - Adding a Secondary Appliance](#).

8. Appliance Configuration for Philips IntelliSpace PACS – Using Layer 7 SNAT Mode

8.1. Configuring the External Health Check Scripts

Once configured, these health checks will be available when configuring the VIPs.

8.1.1. Ping Check

1. Using the WebUI, navigate to *Cluster Configuration > Health Check Scripts* and click **Add New Health Check**.

Health Check Details		
Name:	Ping-Check	?
Type:	Virtual Service	?
Template:	ping.sh	?

2. Specify an appropriate **Name** for the health check, e.g. **Ping-Check**.
3. Set **Type** to **Virtual Service**.
4. Set **Template** to **ping.sh**.
5. Click **Update**.

8.1.2. MS-SQL Check

The Microsoft SQL health check requires the Microsoft ODBC Driver. Because it is not free and open source software, this driver cannot be redistributed with our load balancer. We have a blog post on our website which walks through how to set up and use this health check. This blog post is available here:

<https://www.loadbalancer.org/blog/ms-sql-health-check/>. Once this has been completed, follow the steps below to complete the process.



1. Using the WebUI, navigate to *Cluster Configuration > Health Check Scripts* and click **Add New Health Check**.

Health Check Details	
Name:	ms-sql-check
Type:	Virtual Service
Template:	ms-sql-check

2. Specify an appropriate **Name** for the health check, e.g. **ms-sql-check**.
3. Set **Type** to **Virtual Service**.
4. Set **Template** to **ms-sql-check**.
5. Click **Update**.

8.2. Configuring VIP 1 – DICOM

8.2.1. 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. **DICOM**.
3. Set the **Virtual Service IP Address** field to the required IP address, e.g. **192.168.85.5**.
4. Set the **Ports** field to **104**.
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	DICOM	?
IP Address	192.168.85.5	?
Ports	104	?

Protocol		
Layer 7 Protocol	TCP Mode	?

7. Click **Modify** next to the newly created VIP.
8. In the **Other** section, click **Advanced** to show more options.
9. Set the **Set Source Address** field to the SNAT IP address needed, e.g. **192.168.85.4**.



10. Click **Update**.

8.2.2. Defining the Real Servers (RIPs)

1. 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.
2. Define the *Label* for the real server as required, e.g. **Server1**.
3. Set the *Real Server IP Address* field to the required IP address, e.g. **10.0.52.10**.
4. Set the *Real Server Port* field to **104**.
5. Click **Update**.
6. Repeat these steps to add additional real servers as required.

Layer 7 Add a new Real Server - DICOM

Label	<input type="text" value="Server1"/>	?
Real Server IP Address	<input type="text" value="10.0.52.10"/>	?
Real Server Port	<input type="text" value="104"/>	?
Re-Encrypt to Backend	<input type="checkbox"/>	?
Weight	<input type="text" value="100"/>	?
		Cancel Update

8.3. Configuring VIP 2 – DICOM Secure

8.3.1. 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. **DICOM-Secure**.
3. Set the *Virtual Service IP Address* field to the required IP address, e.g. **192.168.85.5**.
4. Set the *Ports* field to **2762**.
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	DICOM-Secure	?
IP Address	192.168.85.5	?
Ports	2762	?
Protocol		
Layer 7 Protocol	TCP Mode	?
		Cancel Update

7. Click **Modify** next to the newly created VIP.
8. In the *Other* section, click **Advanced** to show more options.
9. Set the *Set Source Address* field to the SNAT IP address needed, e.g. **192.168.85.4**.
10. Click **Update**.

8.3.2. Defining the Real Servers (RIPs)

1. 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.
2. Define the *Label* for the real server as required, e.g. **Server1**.
3. Set the *Real Server IP Address* field to the required IP address, e.g. **10.0.52.10**.
4. Set the *Real Server Port* field to **2762**.
5. Click **Update**.
6. Repeat these steps to add additional real servers as required.

Layer 7 Add a new Real Server - DICOM-Secure

Label	Server1	?
Real Server IP Address	10.0.52.10	?
Real Server Port	2762	?
Re-Encrypt to Backend	<input type="checkbox"/>	?
Weight	100	?
		Cancel Update

8.4. Configuring VIP 3 – DMWL

8.4.1. 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. **DMWL**.
3. Set the *Virtual Service IP Address* field to the required IP address, e.g. **192.168.85.5**.
4. Set the *Ports* field to **8104**.
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	DMWL	?
IP Address	192.168.85.5	?
Ports	8104	?
Protocol		
Layer 7 Protocol	TCP Mode	?
		Cancel Update

7. Click **Modify** next to the newly created VIP.
8. In the *Persistence* section, click **Advanced** to show more options.
9. Set the *Persistence Timeout* field to **60**.
10. Set *Health Checks* to **External script**.
11. Set *Check Script* to **Ping-Check**.
12. In the *Other* section, click **Advanced** to show more options.
13. Set the *Set Source Address* field to the SNAT IP address needed, e.g. **192.168.85.4**.
14. Click **Update**.

8.4.2. Defining the Real Servers (RIPs)

1. 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.
2. Define the *Label* for the real server as required, e.g. **Server1**.
3. Set the *Real Server IP Address* field to the required IP address, e.g. **10.0.52.20**.
4. Set the *Real Server Port* field to **8104**.
5. Click **Update**.
6. Repeat these steps to add additional real servers as required.

Layer 7 Add a new Real Server - DMWL

Label	Server1	?
Real Server IP Address	10.0.52.20	?
Real Server Port	8104	?
Re-Encrypt to Backend	<input type="checkbox"/>	?
Weight	100	?
		Cancel Update

8.5. Configuring VIP 4 – DMWL Secure

8.5.1. 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. **DMWL-Secure**.
3. Set the *Virtual Service IP Address* field to the required IP address, e.g. **192.168.85.5**.
4. Set the *Ports* field to **10104**.
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	DMWL-Secure	?
IP Address	192.168.85.5	?
Ports	10104	?
Protocol		
Layer 7 Protocol	TCP Mode	?
		Cancel Update

7. Click **Modify** next to the newly created VIP.
8. In the *Persistence* section, click **Advanced** to show more options.
9. Set the *Persistence Timeout* field to **60**.
10. Set *Health Checks* to **External script**.
11. Set *Check Script* to **Ping-check**.



12. In the *Other* section, click **Advanced** to show more options.
13. Set the **Set Source Address** field to the SNAT IP address needed, e.g. **192.168.85.4**.
14. Click **Update**.

8.5.2. Defining the Real Servers (RIPs)

1. 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.
2. Define the *Label* for the real server as required, e.g. **Server1**.
3. Set the *Real Server IP Address* field to the required IP address, e.g. **10.0.52.20**.
4. Set the *Real Server Port* field to **10104**.
5. Click **Update**.
6. Repeat these steps to add additional real servers as required.

Layer 7 Add a new Real Server - DMWL-Secure

Label	Server1	?
Real Server IP Address	10.0.52.20	?
Real Server Port	10104	?
Re-Encrypt to Backend	<input type="checkbox"/>	?
Weight	100	?
		Cancel Update

8.6. Configuring VIP 5 – SQL

8.6.1. 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. **SQL**.
3. Set the *Virtual Service IP Address* field to the required IP address, e.g. **192.168.85.8**.
4. Set the *Ports* field to **1433**.
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	SQL	?
IP Address	192.168.85.8	?
Ports	1433	?
Protocol		
Layer 7 Protocol	TCP Mode	?
		Cancel Update

7. Click **Modify** next to the newly created VIP.
8. In the **Persistence** section, click **Advanced** to show more options.
9. Set the **Persistence Timeout** field to **2**.
10. Set **Health Checks** to **External script**.
11. Set **Check Script** to **ms-sql-check**.

The Microsoft SQL health check requires the Microsoft ODBC Driver. Because it is not free and open source software, this driver cannot be redistributed with our load balancer.

Note

We have a blog post on our website which walks through how to set up and use this health check. This blog post is available here: <https://www.loadbalancer.org/blog/ms-sql-health-check/>. These steps must be completed first before the SQL check is available for selection in the WebUI.

12. In the **Other** section, click **Advanced** to show more options.
13. Set the **Set Source Address** field to the SNAT IP address needed, e.g. **192.168.85.4**.
14. Click **Update**.

8.6.2. Defining the Real Servers (RIPs)

1. 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.
2. Define the **Label** for the real server as required, e.g. **Server1**.
3. Set the **Real Server IP Address** field to the required IP address, e.g. **10.0.52.30**.
4. Set the **Real Server Port** field to **1433**.
5. Click **Update**.
6. Repeat these steps to add additional real servers as required.



Layer 7 Add a new Real Server - SQL

Label	Server1	?
Real Server IP Address	10.0.52.30	?
Real Server Port	1433	?
Re-Encrypt to Backend	<input type="checkbox"/>	?
Weight	100	?
Cancel Update		

8.7. Configuring VIP 6 – LDAP

8.7.1. 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. **LDAP**.
3. Set the *Virtual Service IP Address* field to the required IP address, e.g. **192.168.85.8**.
4. Set the *Ports* field to **3890**.
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	LDAP	?
IP Address	192.168.85.8	?
Ports	3890	?
Protocol		
Layer 7 Protocol	TCP Mode	?
Cancel Update		

7. Click **Modify** next to the newly created VIP.
8. In the *Persistence* section, click **Advanced** to show more options.
9. Set the *Persistence Timeout* field to **2**.
10. In the *Other* section, click **Advanced** to show more options.
11. Set the *Set Source Address* field to the SNAT IP address needed, e.g. **192.168.85.4**.



12. Click **Update**.

8.7.2. Defining the Real Servers (RIPs)

1. 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.
2. Define the *Label* for the real server as required, e.g. **Server1**.
3. Set the *Real Server IP Address* field to the required IP address, e.g. **10.0.52.40**.
4. Set the *Real Server Port* field to **3890**.
5. Click **Update**.
6. Repeat these steps to add additional real servers as required.

Layer 7 Add a new Real Server - LDAP

Label	<input type="text" value="Server1"/>	?
Real Server IP Address	<input type="text" value="10.0.52.40"/>	?
Real Server Port	<input type="text" value="3890"/>	?
Re-Encrypt to Backend	<input type="checkbox"/>	?
Weight	<input type="text" value="100"/>	?
		Cancel Update

8.8. Configuring VIP 6 – LDAP Secure (LDAPS)

8.8.1. 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. **LDAP-Secure**.
3. Set the *Virtual Service IP Address* field to the required IP address, e.g. **192.168.85.8**.
4. Set the *Ports* field to **6360**.
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	LDAP-Secure	?
IP Address	192.168.85.8	?
Ports	6360	?
Protocol		
Layer 7 Protocol	TCP Mode	?
		<input type="button" value="Cancel"/> <input type="button" value="Update"/>

7. Click **Modify** next to the newly created VIP.
8. In the **Persistence** section, click **Advanced** to show more options.
9. Set the **Persistence Timeout** field to **2**.
10. In the **Other** section, click **Advanced** to show more options.
11. Set the **Set Source Address** field to the SNAT IP address needed, e.g. **192.168.85.4**.
12. Click **Update**.

8.8.2. Defining the Real Servers (RIPs)

1. 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.
2. Define the *Label* for the real server as required, e.g. **Server1**.
3. Set the *Real Server IP Address* field to the required IP address, e.g. **10.0.52.40**.
4. Set the *Real Server Port* field to **6360**.
5. Click **Update**.
6. Repeat these steps to add additional real servers as required.

Layer 7 Add a new Real Server - LDAP-Secure

Label	Server1	?
Real Server IP Address	10.0.52.40	?
Real Server Port	6360	?
Re-Encrypt to Backend	<input type="checkbox"/>	?
Weight	100	?
		<input type="button" value="Cancel"/> <input type="button" value="Update"/>



8.9. Configuring VIP 7 – QRSCP

8.9.1. 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. **QRSCP**.
3. Set the *Virtual Service IP Address* field to the required IP address, e.g. **192.168.85.5**.
4. Set the *Ports* field to **107**.
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	QRSCP	?
IP Address	192.168.85.5	?
Ports	107	?
Protocol		
Layer 7 Protocol	TCP Mode	?
		Cancel Update

7. Click **Modify** next to the newly created VIP.
8. In the *Persistence* section, click **Advanced** to show more options.
9. Set the *Persistence Timeout* field to **2**.
10. Set *Health Checks* to **External script**.
11. Set *Check Script* to **Ping-Check**.
12. In the *Other* section, click **Advanced** to show more options.
13. Set the *Set Source Address* field to the SNAT IP address needed, e.g. **192.168.85.4**.
14. Click **Update**.

8.9.2. Defining the Real Servers (RIPs)

1. 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.
2. Define the *Label* for the real server as required, e.g. **Server1**.
3. Set the *Real Server IP Address* field to the required IP address, e.g. **10.0.52.50**.
4. Set the *Real Server Port* field to **107**.



5. Click **Update**.
6. Repeat these steps to add additional real servers as required.

Layer 7 Add a new Real Server - QRSCP

Label	Server1	?
Real Server IP Address	10.0.52.50	?
Real Server Port	107	?
Re-Encrypt to Backend	<input type="checkbox"/>	?
Weight	100	?
<input type="button" value="Cancel"/> <input type="button" value="Update"/>		

8.10. Configuring VIP 8 – QRSCP Secure

8.10.1. 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. **QRSCP-Secure**.
3. Set the *Virtual Service IP Address* field to the required IP address, e.g. **192.168.85.5**.
4. Set the *Ports* field to **2765**.
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	QRSCP-Secure	?
IP Address	192.168.85.5	?
Ports	2765	?
Protocol		
Layer 7 Protocol	TCP Mode	?
		<input type="button" value="Cancel"/> <input type="button" value="Update"/>

7. Click **Modify** next to the newly created VIP.
8. In the *Persistence* section, click **Advanced** to show more options.
9. Set the *Persistence Timeout* field to **2**.



10. Set **Health Checks** to **External script**.
11. Set **Check Script** to **Ping-Check**.
12. In the **Other** section, click **Advanced** to show more options.
13. Set the **Set Source Address** field to the SNAT IP address needed, e.g. **192.168.85.4**.
14. Click **Update**.

8.10.2. Defining the Real Servers (RIPs)

1. 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.
2. Define the **Label** for the real server as required, e.g. **Server1**.
3. Set the **Real Server IP Address** field to the required IP address, e.g. **10.0.52.50**.
4. Set the **Real Server Port** field to **2765**.
5. Click **Update**.
6. Repeat these steps to add additional real servers as required.

Layer 7 Add a new Real Server - QRSCP-Secure

Label	Server1	?
Real Server IP Address	10.0.52.50	?
Real Server Port	2765	?
Re-Encrypt to Backend	<input type="checkbox"/>	?
Weight	100	?
		Cancel Update

8.11. 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 Philips IntelliSpace servers) and shows the state/health of each server as well as the state of each cluster as a whole. The example below shows that all Philips servers are healthy and available to accept connections.

SYSTEM OVERVIEW 									2018-08-07 16:45:13 UTC
VIRTUAL SERVICE	IP	PORTS	CONNNS	PROTOCOL	METHOD	MODE			
 DICOM	192.168.85.5	104	0	TCP	Layer 7	Proxy			
REAL SERVER	IP	PORTS	WEIGHT	CONNNS					
 Server1	10.0.52.10	104	100	0	Drain	Halt			
 Server2	10.0.52.10	104	100	0	Drain	Halt			
 DICOM-Secure	192.168.85.5	2762	0	TCP	Layer 7	Proxy			
 DMWL	192.168.85.5	8104	0	TCP	Layer 7	Proxy			
 DMWL-Secure	192.168.85.5	10104	0	TCP	Layer 7	Proxy			
 SQL	192.168.85.8	1433	0	TCP	Layer 7	Proxy			
REAL SERVER	IP	PORTS	WEIGHT	CONNNS					
 Server1	10.0.52.30	1433	100	0	Drain	Halt			
 Server2	10.0.52.30	1433	100	0	Drain	Halt			
 LDAP	192.168.85.8	3890	0	TCP	Layer 7	Proxy			
 LDAP-Secure	192.168.85.8	6360	0	TCP	Layer 7	Proxy			
 QRSCP	192.168.85.5	107	0	TCP	Layer 7	Proxy			
 QRSCP-Secure	192.168.85.5	2765	0	TCP	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 Outbound SNAT Rules for DICOM Services (iExport and iQuery)

iptables SNAT rules can be used to SNAT traffic coming from the real servers that is destined to specific ports. To make sure that these rules do not affect other traffic, the rules should be restricted so that they only apply to traffic that has a source IP address matching a real server that requires this configuration.

It is important to note that **the real servers in question must use the load balancer as their default gateway** in order for SNAT rules as described here to function.

It is recommended to put the SNAT rules in the load balancer's firewall script. This can be edited from the WebUI under *Maintenance > Firewall Script*. Any changes made here must also be made on the Secondary load balancer, if present, as these changes are manual and are not synchronised automatically.

12.1.1. Example SNAT rule

```
iptables -t nat -A POSTROUTING -p tcp -s <real server IP address> -m multiport --dports 104,11112  
-j SNAT --to-source <SNAT IP address>
```

12.1.2. Example SNAT rule using multiple IP addresses

```
iptables -t nat -A POSTROUTING -p tcp -s 10.10.5.59,10.10.5.60,10.10.5.113 -m multiport --dports  
104,11112 -j SNAT --to-source 10.10.5.100
```

 Note

The SNAT rules need to be adjusted to accommodate the customer configured destination TCP port for each iExport and iQuery destination.

12.2. Source IP Transparency at Layer 7 Using TPROXY

Layer 7 is the recommended load balancing method for Philips IntelliSpace PACS. Load balancing at layer 7 uses the HAProxy service. HAProxy is a proxy which means that a new connection is established from the proxy out to the backend server in response to an inbound client connection to the proxy. This means that the source IP address of the packet reaching the server will be the proxy's address. By default this is the IP address assigned to the load balancer's Ethernet interface.

The TProxy (Transparent Proxy) kernel option can be used alongside HAProxy to enable IP address transparency, i.e. maintain the actual source IP address of the client. When enabling TProxy, it is important to be aware of the topology requirements for it to work correctly.

Layer 7 SNAT mode with TProxy is typically used in a 2-arm configuration where the VIP is located in one subnet and the load balanced Real Servers are located in another. This can be achieved by using two network adapters, or by creating VLAN's on a single adapter. Single arm configuration is also supported under certain conditions - for more information please refer to [Transparency at Layer 7](#).

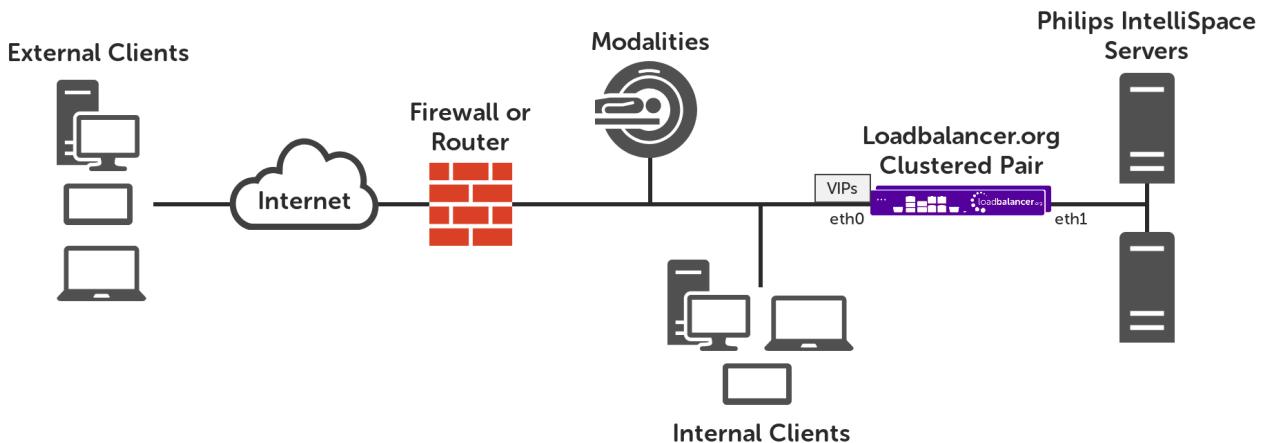
The default gateway on the Real Servers must be an IP address on the load balancer - for a clustered pair, this



should be a floating IP to allow it to move between appliances when needed.

Using a 2-arm Topology:

The diagram below is an overview of a network layout where the Philips IntelliSpace servers sit in their own separate subnet.



12.3. 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.

12.3.1. 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



WebUI Main Menu Option	Sub Menu Option	Description
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	Firewall Script	Firewall (iptables) configuration
Maintenance	Firewall Lockdown Wizard	Appliance management lockdown settings

① Important

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

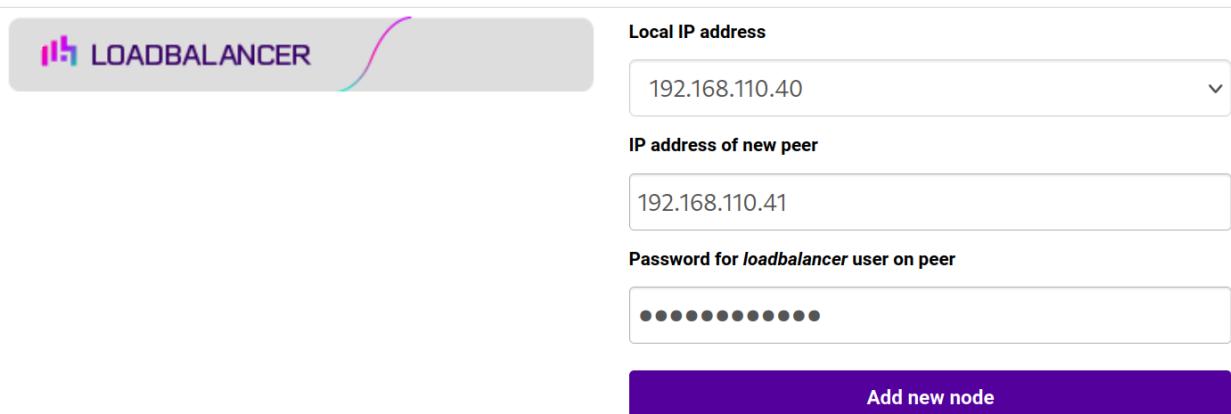
12.3.2. Configuring the HA Clustered Pair

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

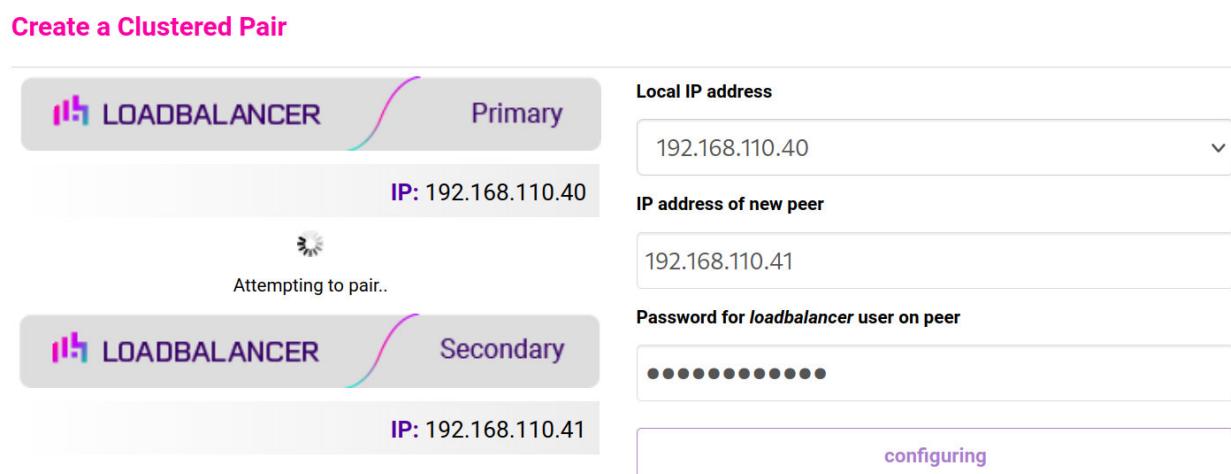


The screenshot shows the 'Create a Clustered Pair' page. At the top, there's a logo for 'LOADBALANCER'. Below it, there are four input fields: 'Local IP address' containing '192.168.110.40', 'IP address of new peer' containing '192.168.110.41', and 'Password for loadbalancer user on peer' (redacted). At the bottom right is a blue button labeled 'Add new node'.

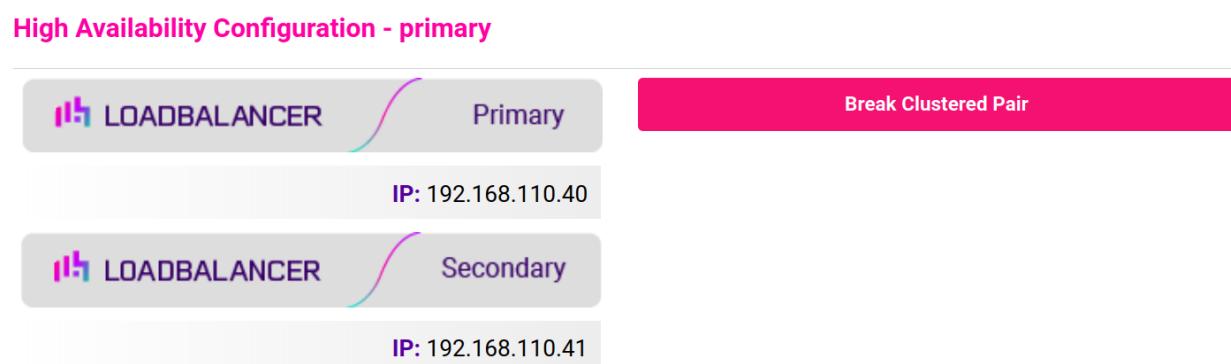
3. Specify the IP address and the *loadbalancer* user's password for the Secondary (peer) appliance as shown in the example above.



4. Click **Add new node**.
5. The pairing process now commences as shown below:



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



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](#).



13. Document Revision History

Version	Date	Change	Reason for Change	Changed By
1.0.0	16 August 2018	Initial version		AH
1.0.1	6 December 2018	Added the new "Company Contact Information" page	Required updates	AH
1.1.0	10 December 2019	Styling and layout	General styling updates	AH
1.1.1	18 December 2019	Added the section "Finalizing the Configuration" to ensure HAProxy is explicitly reloaded	Provided clarity for reloading HAProxy post-configuration	AH
1.1.2	21 August 2020	New title page Updated Canadian contact details New screenshots for creating layer 7 VIPs Amended instructions for configuring persistence timeouts and the layer 7 source address	Branding update Change to Canadian contact details Changes to the appliance WebUI	AH
1.2.0	1 January 2022	Converted the document to AsciiDoc	Move to new documentation system	AH, RJC, ZAC
1.2.1	12 May 2022	Updated external health check 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



Version	Date	Change	Reason for Change	Changed By
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





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://www.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.

