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
       Main Menu Options .................................................. 8
   7.4. Appliance Software Update ........................................ 9
       Determining the Current Software Version ......................... 9
       Checking for Updates using Online Update ....................... 9
       Using Offline Update .............................................. 10
   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
       Ping Check ......................................................... 11
       MS-SQL Check .................................................... 11
   8.2. Configuring VIP 1 – DICOM ....................................... 12
       Configuring the Virtual Service (VIP) ............................ 12
       Defining the Real Servers (RIPs) ................................ 13
   8.3. Configuring VIP 2 – DICOM Secure ................................ 13
       Configuring the Virtual Service (VIP) ............................ 13
       Defining the Real Servers (RIPs) ................................ 14
   8.4. Configuring VIP 3 – DMWL ......................................... 14
       Configuring the Virtual Service (VIP) ............................ 14
       Defining the Real Servers (RIPs) ................................ 15
   8.5. Configuring VIP 4 – DMWL Secure ................................ 16
       Configuring the Virtual Service (VIP) ............................ 16
       Defining the Real Servers (RIPs) ................................ 17
   8.6. Configuring VIP 5 – SQL ........................................... 17
       Configuring the Virtual Service (VIP) ............................ 17
       Defining the Real Servers (RIPs) ................................ 18
   8.7. Configuring VIP 6 – LDAP .......................................... 19
       Configuring the Virtual Service (VIP) ............................ 19
       Defining the Real Servers (RIPs) ................................ 20
   8.8. Configuring VIP 6 – LDAP Secure (LDAPS) ....................... 20
       Configuring the Virtual Service (VIP) ............................ 20
<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Defining the Real Servers (RIPs)</td>
<td>21</td>
</tr>
<tr>
<td>8.9. Configuring VIP 7 – QRSCP</td>
<td>22</td>
</tr>
<tr>
<td>Configuring the Virtual Service (VIP)</td>
<td>22</td>
</tr>
<tr>
<td>Defining the Real Servers (RIPs)</td>
<td>22</td>
</tr>
<tr>
<td>8.10. Configuring VIP 8 – QRSCP Secure</td>
<td>23</td>
</tr>
<tr>
<td>Configuring the Virtual Service (VIP)</td>
<td>23</td>
</tr>
<tr>
<td>Defining the Real Servers (RIPs)</td>
<td>24</td>
</tr>
<tr>
<td>8.11. Finalizing the Configuration</td>
<td>24</td>
</tr>
<tr>
<td>9. Testing &amp; Verification</td>
<td>24</td>
</tr>
<tr>
<td>9.1. Using System Overview</td>
<td>25</td>
</tr>
<tr>
<td>10. Technical Support</td>
<td>25</td>
</tr>
<tr>
<td>11. Further Documentation</td>
<td>25</td>
</tr>
<tr>
<td>12. Appendix</td>
<td>26</td>
</tr>
<tr>
<td>12.1. Configuring Outbound SNAT Rules for DICOM Services (iExport and iQuery)</td>
<td>26</td>
</tr>
<tr>
<td>Example SNAT rule</td>
<td>26</td>
</tr>
<tr>
<td>Example SNAT rule using multiple IP addresses</td>
<td>26</td>
</tr>
<tr>
<td>12.2. Source IP Transparency at Layer 7 Using TPROXY</td>
<td>26</td>
</tr>
<tr>
<td>12.3. Configuring HA - Adding a Secondary Appliance</td>
<td>27</td>
</tr>
<tr>
<td>Non-Replicated Settings</td>
<td>27</td>
</tr>
<tr>
<td>Configuring the HA Clustered Pair</td>
<td>28</td>
</tr>
<tr>
<td>13. Document Revision History</td>
<td>30</td>
</tr>
</tbody>
</table>
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.

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

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

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:

<table>
<thead>
<tr>
<th>Port</th>
<th>Protocols</th>
<th>Use</th>
</tr>
</thead>
<tbody>
<tr>
<td>104</td>
<td>TCP/DICOM</td>
<td>DICOM traffic</td>
</tr>
<tr>
<td>2762</td>
<td>TCP/TLS/DICOM</td>
<td>DICOM traffic over TLS, &quot;DICOM secure&quot;</td>
</tr>
<tr>
<td>8104</td>
<td>TCP/DICOM</td>
<td>DMWL traffic (DICOM Modality Worklists) traffic</td>
</tr>
<tr>
<td>10104</td>
<td>TCP/TLS/DICOM</td>
<td>DMWL traffic over TLS, &quot;DMWL secure&quot;</td>
</tr>
<tr>
<td>1433</td>
<td>TCP/SQL</td>
<td>MS SQL service</td>
</tr>
<tr>
<td>3890</td>
<td>TCP/LDAP</td>
<td>LDAP service</td>
</tr>
<tr>
<td>6360</td>
<td>TCP/LDAPS</td>
<td>Secure LDAP service</td>
</tr>
<tr>
<td>107</td>
<td>TCP/DICOM</td>
<td>QRSCP service (Query/Retrieve Service Class Provider)</td>
</tr>
<tr>
<td>2765</td>
<td>TCP/TLS/DICOM</td>
<td>QRSCP service over TLS, &quot;QRSCP secure&quot;</td>
</tr>
</tbody>
</table>

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

VIP = Virtual IP 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. 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
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 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.

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

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:


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:

3. 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, RIPv 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 & RIPv

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

**View Configuration** - Display the saved appliance configuration settings
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:

Checking for Updates using Online Update

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.

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:

   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:

<table>
<thead>
<tr>
<th>Protocol</th>
<th>Port</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>TCP</td>
<td>22 *</td>
<td>SSH</td>
</tr>
<tr>
<td>TCP &amp; UDP</td>
<td>53 *</td>
<td>DNS / GSLB</td>
</tr>
<tr>
<td>TCP</td>
<td>123</td>
<td>NTP</td>
</tr>
<tr>
<td>TCP &amp; UDP</td>
<td>161 *</td>
<td>SNMP</td>
</tr>
<tr>
<td>UDP</td>
<td>6694</td>
<td>Heartbeat between Primary &amp; Secondary appliances in HA mode</td>
</tr>
<tr>
<td>TCP</td>
<td>7778</td>
<td>HAProxy persistence table replication</td>
</tr>
<tr>
<td>TCP</td>
<td>9000 *</td>
<td>Gateway service (Centralized/Portal Management)</td>
</tr>
</tbody>
</table>
### Protocol | Port | Purpose
---|---|---
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.

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.

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

   ![Health Check Details](image)
   - **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*.

**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

#### 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]

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.

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.

8.3. Configuring VIP 2 – DICOM Secure

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

<table>
<thead>
<tr>
<th>Virtual Service</th>
<th>[Advanced +]</th>
</tr>
</thead>
<tbody>
<tr>
<td>Label</td>
<td>DICOM-Secure</td>
</tr>
<tr>
<td>IP Address</td>
<td>192.168.85.5</td>
</tr>
<tr>
<td>Ports</td>
<td>2762</td>
</tr>
<tr>
<td>Layer 7 Protocol</td>
<td>TCP Mode</td>
</tr>
</tbody>
</table>

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**.

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.

8.4. Configuring VIP 3 – DMWL

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.

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**.

**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.
8.5. Configuring VIP 4 – DMWL Secure

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.

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.

**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.

8.6. Configuring VIP 5 – SQL

**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.
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/](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**.

**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.
8.7. Configuring VIP 6 – LDAP

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.

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.

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.

8.8. Configuring VIP 6 – LDAP Secure (LDAPS)

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

1. Click **Modify** next to the newly created VIP.
2. In the **Persistence** section, click **Advanced** to show more options.
3. Set the **Persistence Timeout** field to 2.
4. In the **Other** section, click **Advanced** to show more options.
5. Set the **Set Source Address** field to the SNAT IP address needed, e.g. 192.168.85.4.
6. Click **Update**.

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.
8.9. Configuring VIP 7 – QRSCP

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.

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.

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.

8.10. Configuring VIP 8 – QRSCP Secure

**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.

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.

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.

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 & RIPv (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.

<table>
<thead>
<tr>
<th>VIRTUAL SERVICE</th>
<th>IP</th>
<th>PORTS</th>
<th>CONNS</th>
<th>PROTOCOL</th>
<th>METHOD</th>
<th>MODE</th>
</tr>
</thead>
<tbody>
<tr>
<td>DICOM</td>
<td>192.168.85.5</td>
<td>104</td>
<td>0</td>
<td>TCP</td>
<td>Layer 7</td>
<td>Proxy</td>
</tr>
<tr>
<td>Server1</td>
<td>10.0.52.10</td>
<td>104</td>
<td>100</td>
<td>0</td>
<td>Drain</td>
<td>Halt</td>
</tr>
<tr>
<td>Server2</td>
<td>10.0.52.10</td>
<td>104</td>
<td>100</td>
<td>0</td>
<td>Drain</td>
<td>Halt</td>
</tr>
<tr>
<td>DICOM-Secure</td>
<td>192.168.85.5</td>
<td>2762</td>
<td>0</td>
<td>TCP</td>
<td>Layer 7</td>
<td>Proxy</td>
</tr>
<tr>
<td>DMWL</td>
<td>192.168.85.5</td>
<td>8104</td>
<td>0</td>
<td>TCP</td>
<td>Layer 7</td>
<td>Proxy</td>
</tr>
<tr>
<td>DMWL-Secure</td>
<td>192.168.85.5</td>
<td>10104</td>
<td>0</td>
<td>TCP</td>
<td>Layer 7</td>
<td>Proxy</td>
</tr>
<tr>
<td>SQL</td>
<td>192.168.85.8</td>
<td>1433</td>
<td>0</td>
<td>TCP</td>
<td>Layer 7</td>
<td>Proxy</td>
</tr>
<tr>
<td>Server1</td>
<td>10.0.52.30</td>
<td>1433</td>
<td>100</td>
<td>0</td>
<td>Drain</td>
<td>Halt</td>
</tr>
<tr>
<td>Server2</td>
<td>10.0.52.30</td>
<td>1433</td>
<td>100</td>
<td>0</td>
<td>Drain</td>
<td>Halt</td>
</tr>
<tr>
<td>LDAP</td>
<td>192.168.85.8</td>
<td>3890</td>
<td>0</td>
<td>TCP</td>
<td>Layer 7</td>
<td>Proxy</td>
</tr>
<tr>
<td>LDAP-Secure</td>
<td>192.168.85.8</td>
<td>6360</td>
<td>0</td>
<td>TCP</td>
<td>Layer 7</td>
<td>Proxy</td>
</tr>
<tr>
<td>QRSCP</td>
<td>192.168.85.5</td>
<td>107</td>
<td>0</td>
<td>TCP</td>
<td>Layer 7</td>
<td>Proxy</td>
</tr>
<tr>
<td>QRSCP-Secure</td>
<td>192.168.85.5</td>
<td>2765</td>
<td>0</td>
<td>TCP</td>
<td>Layer 7</td>
<td>Proxy</td>
</tr>
</tbody>
</table>

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.

**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>
```

**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.

![Network Diagram](image)

### 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.

### 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:

<table>
<thead>
<tr>
<th>WebUI Main Menu Option</th>
<th>Sub Menu Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Local Configuration</td>
<td>Hostname &amp; DNS</td>
<td>Hostname and DNS settings</td>
</tr>
<tr>
<td>Local Configuration</td>
<td>Network Interface Configuration</td>
<td>Interface IP addresses, bonding configuration and VLANs</td>
</tr>
<tr>
<td>Local Configuration</td>
<td>Routing</td>
<td>Default gateways and static routes</td>
</tr>
<tr>
<td>Local Configuration</td>
<td>System Date &amp; time</td>
<td>Time and date related settings</td>
</tr>
</tbody>
</table>
### Configuring the HA Clustered Pair

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**.

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

### 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.

### Create a Clustered Pair

- **Local IP address**: 192.168.110.40
- **IP address of new peer**: 192.168.110.41
- **Password for loadbalancer user on peer**: ************
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](image)

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

![High Availability Configuration - primary](image)

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

<table>
<thead>
<tr>
<th>Version</th>
<th>Date</th>
<th>Change</th>
<th>Reason for Change</th>
<th>Changed By</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.0.0</td>
<td>16 August 2018</td>
<td>Initial version</td>
<td></td>
<td>AH</td>
</tr>
<tr>
<td>1.0.1</td>
<td>6 December 2018</td>
<td>Added the new &quot;Company Contact Information&quot; page</td>
<td>Required updates</td>
<td>AH</td>
</tr>
<tr>
<td>1.1.0</td>
<td>10 December 2019</td>
<td>Styling and layout</td>
<td>General styling updates</td>
<td>AH</td>
</tr>
<tr>
<td>1.1.1</td>
<td>18 December 2019</td>
<td>Added the section &quot;Finalizing the Configuration&quot; to ensure HAProxy is explicitly reloaded</td>
<td>Provided clarity for reloading HAProxy post-configuration</td>
<td>AH</td>
</tr>
<tr>
<td>1.1.2</td>
<td>21 August 2020</td>
<td>New title page</td>
<td>Branding update</td>
<td>AH</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Updated Canadian contact details</td>
<td>Change to Canadian contact details</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>New screenshots for creating layer 7 VIPs</td>
<td>Changes to the appliance WebUI</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Amended instructions for configuring persistence timeouts and the layer 7 source address</td>
<td></td>
<td></td>
</tr>
<tr>
<td>1.2.0</td>
<td>1 January 2022</td>
<td>Converted the document to AsciiDoc</td>
<td>Move to new documentation system</td>
<td>AH, RJC, ZAC</td>
</tr>
<tr>
<td>1.2.1</td>
<td>12 May 2022</td>
<td>Updated external health check related content to reflect latest software version</td>
<td>New software release</td>
<td>RJC</td>
</tr>
<tr>
<td>1.2.2</td>
<td>28 September 2022</td>
<td>Updated layer 7 VIP and RIP creation screenshots</td>
<td>Reflect changes in the web user interface</td>
<td>AH</td>
</tr>
<tr>
<td>1.2.3</td>
<td>5 January 2023</td>
<td>Combined software version information into one section</td>
<td>Housekeeping across all documentation</td>
<td>AH</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Added one level of section numbering</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Added software update instructions</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Added table of ports used by the appliance</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Reworded 'Further Documentation' section</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Removed references to the colour of certain UI elements</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Version</td>
<td>Date</td>
<td>Change</td>
<td>Reason for Change</td>
<td>Changed By</td>
</tr>
<tr>
<td>---------</td>
<td>--------------------</td>
<td>---------------------------------------------</td>
<td>------------------------------------</td>
<td>------------</td>
</tr>
<tr>
<td>1.2.4</td>
<td>2 February 2023</td>
<td>Updated screenshots</td>
<td>Branding update</td>
<td>AH</td>
</tr>
<tr>
<td>1.2.5</td>
<td>7 March 2023</td>
<td>Removed conclusion section</td>
<td>Updates across all documentation</td>
<td>AH</td>
</tr>
<tr>
<td>1.3.0</td>
<td>24 March 2023</td>
<td>New document theme</td>
<td>Branding update</td>
<td>AH</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Modified diagram colours</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
About Loadbalancer.org

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